
MASTER THESIS

Promoting information secure behaviour in an organizational context.

Two field experiments on the topic of phishing and screen locking

Jeroen De Bruin, J.C.

Student number: 416037

Erasmus School of Economics, Erasmus University Rotterdam, Rotterdam, the Netherlands
MSC Economics and Business, Behavioural economics, master specialization in Marketing

I N F O

Supervisor: *Ilke Aydogan*

Handed in: 21-06-2016

Keywords: *security education, training and awareness programs; information security policy compliance; information provision; previous experience; constant salient reminders; determinants for information (in)secure behaviour*

ABSTRACT

Employees play an important role in the information security performance of organizations by their security awareness, cautious behaviour and compliance with policies and procedures. In this thesis we study the effect of security training and awareness programs on individuals' information (in)secure behaviour. At first, we analysed the determinants of information (in)secure behaviour, their experience and personal role in information security. In two field experiments, concerning phishing and screen locking, we tested the impact of information provision, simulating experience with phishing mails and constant salient reminders on improvements of information secure behaviour. Participants in the experiments were employees of the Dutch Ministry of Economic Affairs.

The main finding of this study is, that in both experiments all three treatments were effective in improving information secure behaviour. Furthermore, we found interventions in the screen locking experiment to be effective up to two months after treatments were stopped. This study therefore supports effectiveness of interventions based upon behavioural insights, applied to the domain of information security. Furthermore, by comparing effectiveness of interventions, this thesis provides both practitioners as scientists, clear actionable means which should be taken into account for developing security education, training and awareness programs. Although all treatments improved information secure behaviour, results also indicate that in order to be successful, trainings and awareness campaigns should be repeated.

Preface

Commissioned by Operational management of the Dutch ministry of Economic Affairs, the Behavioural Insights Team of EZ (BIT EZ (AEP)) was asked to test how behavioural insights can help to promote information secure behaviour. Information security plays an important role in all processes within EZ and covers various aspects and behaviours. This involves, among other things; not sharing passwords, dealing with sensitive information and not to use private mail to send (sensitive) files. Based on an assessment of the extent and / or impact of the problems, and also the measurability and feasibility of (desired) behaviour, we have chosen to focus on two topics;

- Screen locking (manually)
- Phishing

Table of contents

MASTER THESIS	i
Preface	ii
Table of contents.....	iii
Table overview.....	viii
Figure overview	vii
Chapter 1: Introduction	1
1.1 The research question	2
1.1.1 Phishing	3
1.1.2 Screen locking	3
1.2 Field experiments.....	3
1.3 The contribution of this thesis.....	4
1.3.1 Practical relevance.....	4
1.3.2 Scientific relevance.....	4
1.4 Structure	5
Chapter 2: Literature overview	6
2.1 Determinants of information (in)secure behaviour	6
2.1.1 Screen locking	7
2.1.2 Phishing emails	9
2.2 Training Employees – The effect of Information, (Personal) Experience and Reminders.....	12
2.2.1 Security education, training and awareness programs (SETA)	12
2.2.2 The effect of Information Provision	13
2.2.3 The effect of (Personal) Experience & Feedback.....	16
2.2.4 The effect of emphasizing desired behaviour	18
2.3. Research question & Hypotheses.....	21
2.3.1 Phishing	21
2.3.2 Screen locking	22

Chapter 3: Research Methods	24
3.1 Phishing Mail	24
3.1.1 Participants.....	24
3.1.2 Design	24
3.1.3 Group formation.....	25
3.1.4 Procedure.....	26
3.2 Screen locking	30
3.2.1 Participants.....	30
3.2.2 Design	31
3.2.3 Group formation.....	31
3.2.4 Procedure.....	32
3.3 Recap	34
Chapter 4: Results	36
4.1 Phishing mail.....	36
4.1.1 Contamination of the experiment and implications.....	36
4.1.2 Measuring falling for phishing fraud	36
4.1.3 Demographics:.....	37
4.1.4 First results - Treatments	38
4.1.5 Treatment Differences.....	39
4.1.6 Regression analysis	43
4.1.7 Comparing results with & without the exclusion of the NVWA	46
4.1.8 Other results.....	46
4.2. Screen locking	47
4.2.1 Measuring screen locking behaviour.....	47
4.2.2 Manual locks per hour worked.....	47
4.2.3 Ratio of manual locks to total locks.....	50
4.2.4 Regression Analysis	51

Chapter 5: Discussion	59
5.1 Phishing	59
5.1.1 Measurement 1: Participants clicked on the link	59
5.1.2 Measurement 2: Participants filled in passwords	60
5.1.3 General discussion	60
5.2 Screen locking	64
5.2.1 Manual locks per hour & ratio manual locks to total locks	64
5.2.2 Regression analysis	65
5.2.3 General discussion	66
5.3 Implications	69
5.4 Limitations	71
5.5 Future research	72
 Chapter 6: Conclusion	 74
 Appendices	 77
Appendix 3.1. <i>PM</i> : Kruskal-Wallis test results group formation	77
Appendix 3.2. <i>PM</i> : Security notice prior to phishing mail field experiment	78
Appendix 3.3. <i>PM</i> : Standard answers incoming mails and phone calls.....	79
Appendix 3.4. <i>PM</i> : Phishing mail 1 (simulated experience treatment)	83
Appendix 3.5. <i>PM</i> : Website first phishing mail and pop-up screen	84
Appendix 3.6. <i>PM</i> : Short debriefing after first phishing mail	85
Appendix 3.7. <i>PM</i> : Infographics (Information provision treatment).....	86
Appendix 3.8. <i>PM</i> : Phishing mail 2	89
Appendix 3.9. <i>PM</i> : Website second phishing mail and Pop-up screen	90
Appendix 3.10. <i>PM</i> : General debriefing and explanation of the phishing field experiment	91
Appendix 3.11. <i>SL</i> : Group formation Bezuidenhoutseweg 73	95
Appendix 3.12. <i>SL</i> : A5-Flyer (Information provision treatment)	96
Appendix 3.13. <i>SL</i> : Stickers (constant salient remainder treatment)	97

Appendix 4.1. <i>PM</i> : Comparing results of phishing mail experiment, with and without the exclusion of the NVWA	98
Appendix 4.2. <i>PM</i> : Kruskal-Wallis test results (without the NVWA)	103
Appendix 4.3. <i>PM</i> : M2_VisitLinkBIN: Logit regression analysis	104
Appendix 4.4. <i>PM</i> : M2_VisitLinkBIN: Wald- χ^2 test results and Fischer exact and χ^2 -test results (gender & employee contract).	105
Appendix 4.5. <i>PM</i> : M2_VisitLinkBIN: Correlation matrix	106
Appendix 4.6. <i>PM</i> : M2_VisitLinkBIN: Variance Inflation Factor values	107
Appendix 4.7. <i>PM</i> : M2_Password: Logit regression analysis	108
Appendix 4.8. <i>PM</i> : M2_Password: Wald- χ^2 test results , Fischer exact and χ^2 -test results (gender & employee contract).	109
Appendix 4.9. <i>PM</i> : M2_Password: Correlation matrix.....	110
Appendix 4.10. <i>PM</i> : M2_Password: Variance Inflation Factor values	111
Appendix 4.11. <i>SL</i> : Differences in number of observations, average- and total pure working time.....	112
Appendix 4.12. <i>SL</i> : T-test results Per2-Per3, Per2-Per4 and Per3-Per4 comparison of number of times participants manually locked their screen per hour, and the ratio of manual locks to total locks.	113
Appendix 4.13. <i>SL</i> : Main model: Hausman test results	114
Appendix 4.14. <i>SL</i> : Main model: Correlation matrix.....	115
Appendix 4.15. <i>SL</i> : Main model: Variance Inflation Factor values.....	116
Appendix 4.16. <i>SL</i> : Main model: Autocorrelation and heteroscedasticity tests.....	117
Appendix 4.17. <i>SL</i> : Main model: Fixed effects regression analysis.....	118
Appendix 4.18. <i>SL</i> : Main model: Wald-test results	119
Appendix 4.19. <i>SL</i> : Extended model: Hausman test results.....	120
Appendix 4.20. <i>SL</i> : Extended model: Correlation matrix (3 parts).....	121
Appendix 4.21. <i>SL</i> : Extended model: Variance Inflation Factor values	124
Appendix 4.22. <i>SL</i> : Extended model: Autocorrelation and heteroscedasticity tests	125
Appendix 4.23. <i>SL</i> : Extended model: Fixed effects regression analysis	126
Appendix 4.24. <i>SL</i> : Extended model: Wald-test results.....	127
Bibliography	128

Table overview

TABLE 3.1. <i>PM</i> : EXPERIMENTAL DESIGN	24
TABLE 3.2. <i>PM</i> : PHISHING MAIL EXPERIMENTAL PROCEDURE	25
TABLE 3.3. <i>PM</i> : SUMMARY STATISTICS PER GROUP.....	25
TABLE 3.4. <i>SL</i> : SCREEN LOCKING EXPERIMENTAL DESIGN.....	31
TABLE 3.5. <i>SL</i> : SCREEN LOCKING EXPERIMENTAL PROCEDURE.....	31
TABLE 3.6. <i>SL</i> : (AVERAGE OCCUPIED) PC'S PER TREATMENT GROUP.....	31
TABLE 4.1. <i>PM</i> : DEMOGRAPHIC FACTORS OF PARTICIPANTS PER TREATMENT GROUP	37
TABLE 4.2. <i>PM</i> : NUMBER OF PARTICIPANTS FALLING FOR PHISHING FRAUD PER CONDITION (IN EXACT NUMBERS AND PERCENTAGES).	38
TABLE 4.3. <i>PM</i> : OVERVIEW χ^2 TEST RESULTS - PARTICIPANTS VISITED THE LINK IN THE MAIL PER TREATMENT	39
TABLE 4.4. <i>PM</i> : OVERVIEW χ^2 TEST RESULTS - PARTICIPANTS FILLED IN THEIR PASSWORD PER TREATMENT	39
TABLE 4.5. <i>PM</i> : OVERVIEW χ^2 TEST RESULTS- PARTICIPANTS WHO FILLED IN THEIR PASSWORD OF THOSE WHO CLICKED ON THE LINK EMBEDDED IN THE PHISHING MAIL.	40
TABLE 4.6. <i>PM</i> : PARTICIPANTS VISITING THE LINK, PER TREATMENT (IN EXACT NUMBERS AND PERCENTAGES). NUMBER OF OBSERVATIONS, GENDER, AGE, EMPLOYEE CONTRACT AND ORGANIZATIONAL DIVISION DISTRIBUTION.....	41
TABLE 4.7. <i>PM</i> : PARTICIPANTS FILLING IN THEIR PASSWORD, PER TREATMENT (IN EXACT NUMBERS AND PERCENTAGES). NUMBER OF OBSERVATIONS, GENDER, AGE, EMPLOYEE CONTRACT AND ORGANIZATIONAL DIVISION DISTRIBUTION.	42
TABLE 4.8. <i>PM</i> : $Y = M2_VISITLINKBIN$ (VISITED THE SITE). LOGISTIC REGRESSION ANALYSIS WITH PARAMETERS, STANDARD ERRORS, CONFIDENCE INTERVAL, ODDS RATIO'S AND MARGINAL EFFECTS (SIGNIFICANT AT $P < 0,05$).	43
TABLE 4.9. <i>PM</i> : OVERVIEW WALD- χ^2 TEST RESULTS- PARTICIPANTS VISITED THE SITED/ CLICKED ON THE LINK.....	44
TABLE 4.10. <i>PM</i> : $Y = M2_PASSWORD$ (FILLED IN PASSWORD). LOGISTIC REGRESSION ANALYSIS WITH PARAMETERS, STANDARD ERRORS, CONFIDENCE INTERVAL, ODDS RATIO'S AND MARGINAL EFFECTS (SIGNIFICANT AT $P < 0,05$).	45
TABLE 4.11. <i>PM</i> : REGRESSION ANALYSIS- OVERVIEW WALD- χ^2 TEST RESULTS- PARTICIPANTS FILLED IN PASSWORD.....	45
TABLE 4.12. <i>SL</i> : DISTRIBUTION OF AVERAGE PURE WORKING TIME PER TREATMENT GROUP AND PERIOD	47
TABLE 4.13. <i>SL</i> : SUMMARY STATISTICS. MEAN AND STANDARD DEVIATION OF NUMBER OF MANUAL LOCKS PER HOUR WORKED, AND (AVERAGE USED) PC'S PER TREATMENT GROUP...	48
TABLE 4.14. <i>SL</i> : T- TEST RESULTS, NUMBER OF TIMES OF MANUALLY LOCKED SCREENS, INTERVENTION PERIOD, SHORT-TERM POST-TEST AND LONG-TERM POST-TEST COMPARED TO PRE-TEST PERIOD, PER TREATMENT GROUP,	49
TABLE 4.15. <i>SL</i> : SUMMARY STATISTICS. MEAN AND STANDARD DEVIATION OF THE RATIO NUMBER OF MANUAL LOCKS TO TOTAL LOCKS, PER TREATMENT GROUP AND PERIOD.....	51
TABLE 4.16. <i>SL</i> : T-TEST RESULTS, RATIO MANUAL LOCKS TO TOTAL LOCKS: INTERVENTION, SHORT-TERM POST-TEST AND LONG-TERM POST-TEST PERIOD COMPARED TO PRE-TEST PERIOD, PER TREATMENT GROUP	51
TABLE 4.17. <i>SL</i> : TREATMENT IMPACT COMPARISON IN THE INTERVENTION PERIOD.....	52
TABLE 4.18. <i>SL</i> : $Y = HANDLOCK$ (NUMBER OF MANUAL LOCKS), MAIN AND EXTENDED MODEL. FIXED EFFECTS REGRESSION ANALYSIS WITH PARAMETERS AND DRISCOLL-KRAAY STANDARD ERRORS.....	53
TABLE 4.19. <i>SL</i> : TREATMENT IMPACT COMPARISON TWO WEEKS AFTER TREATMENTS WERE STOPPED (SHORT-TERM POST-TEST)	54
TABLE 4.20. <i>SL</i> : TREATMENT IMPACT COMPARISON TWO MONTHS AFTER TREATMENTS WERE STOPPED (LONG-TERM POST-TEST).....	55

TABLE 4.21. <i>SL</i> : TREATMENT IMPACT COMPARISON OF PER2-PER3, PER2-PER4 AND PER3-PER4 – MAIN MODEL.....	55
TABLE 4.22. <i>SL</i> : TREATMENT IMPACT COMPARISON IN THE INTERVENTION PERIOD.....	56
TABLE 4.23. <i>SL</i> : TREATMENT IMPACT COMPARISON TWO WEEKS AFTER TREATMENTS WERE STOPPED (SHORT-TERM POST-TEST).....	56
TABLE 4.24. <i>SL</i> : TREATMENT IMPACT COMPARISON IN THE LONG-TERM POST-TEST PERIOD.....	57
TABLE 4.25. <i>SL</i> : TREATMENT IMPACT COMPARISON OF PER2-PER3, PER2-PER AND PER3-PER4 – EXTENDED MODEL.....	57
TABLE 5.1. <i>PM</i> : SUSCEPTIBILITY TOWARDS PHISHING FRAUD – FULLY, PARTIALLY AND NOT-SUPPORTED HYPOTHESES.....	60
TABLE 5.2. <i>SL</i> : NUMBER OF TIMES PARTICIPANTS MANUALLY LOCKED THEIR SCREENS - FULLY, PARTIALLY AND NON- SUPPORTED HYPOTHESES.....	66
TABLE A.3.1. <i>PM</i> : KRUSKAL-WALLIS EQUALITY-OF-POPULATIONS RANK TEST: AGE.....	77
TABLE A.3.2. <i>PM</i> : KRUSKAL-WALLIS EQUALITY-OF-POPULATIONS RANK TEST: AGE_GROUP.....	77
TABLE A.3.3. <i>PM</i> : KRUSKAL-WALLIS EQUALITY-OF-POPULATIONS RANK TEST: GENDER.....	77
TABLE A.3.4. <i>PM</i> : KRUSKAL-WALLIS EQUALITY-OF-POPULATIONS RANK TEST: INT_EMPLOYEE... ..	77
TABLE A.3.5. <i>PM</i> : KRUSKAL-WALLIS EQUALITY-OF-POPULATIONS RANK TEST: ORGANIZATIONAL SUBDIVISION.....	77
TABLE A.4.1. <i>PM</i> : NUMBER OF PARTICIPANTS FALLING FOR PHISHING FRAUD PER CONDITION (IN EXACT NUMBERS AND PERCENTAGES).....	98
TABLE A.4.2. <i>PM</i> : PERCENTAGE OF PARTICIPANTS WHO CLICKED ON THE EMBEDDED LINK IN THE PHISHING MAIL, DISAGGREGATED PER TREATMENT GROUP AND ORGANIZATIONAL UNIT (WITH THE NVWA INCLUDED).....	99
TABLE A.4.3. <i>PM</i> : PERCENTAGE OF PARTICIPANTS WHO FILLED IN IN PASSWORD DISAGGREGATED, PER TREATMENT GROUP AND ORGANIZATIONAL UNIT (WITH THE NVWA INCLUDED).....	99
TABLE A.4.4. <i>PM</i> : OVERVIEW χ^2 TEST RESULTS - PARTICIPANTS CLICKING ON THE EMBEDDED LINK PER TREATMENT.....	100
TABLE A.4.5. <i>PM</i> : OVERVIEW χ^2 TEST RESULTS - PARTICIPANTS FILLED IN THEIR PASSWORD PER TREATMENT.....	100
TABLE A.4.6. <i>PM</i> : OVERVIEW χ^2 TEST RESULTS- PARTICIPANTS WHO FILLED IN THEIR PASSWORD OF THOSE WHO CLICKED ON THE LINK EMBEDDED IN THE PHISHING MAIL.....	100
TABLE A.4.7. <i>PM</i> : LOGISTIC REGRESSION RESULTS, WITH PARTICIPANTS CLICKED THE EMBEDDED LINK IN THE PHISHING MAIL AS INDEPENDENT VARIABLE (WITH THE NVWA INCLUDED).....	101
TABLE A.4.8. <i>PM</i> : REGRESSION ANALYSIS- OVERVIEW WALD- χ^2 TEST RESULTS: PARTICIPANTS CLICKED ON THE EMBEDDED LINK.....	101
TABLE A.4.9. <i>PM</i> : LOGISTIC REGRESSION RESULTS, WITH PARTICIPANTS FILLED IN THEIR PASSWORD AS INDEPENDENT VARIABLE (WITH THE NVWA INCLUDED).....	102
TABLE A.4.10. <i>PM</i> : REGRESSION ANALYSIS- OVERVIEW WALD- χ^2 TEST RESULTS: PARTICIPANTS FILLED IN PASSWORD.....	102
TABLE A.4.11. <i>PM</i> : KRUSKAL-WALLIS EQUALITY-OF-POPULATIONS RANK TEST: AGE_GROUP ..	103
TABLE A.4.12. <i>PM</i> : KRUSKAL-WALLIS EQUALITY-OF-POPULATIONS RANK TEST: AGE.....	103
TABLE A.4.13. <i>PM</i> : KRUSKAL-WALLIS EQUALITY-OF-POPULATIONS RANK TEST: GENDER.....	103
TABLE A.4.14. <i>PM</i> : KRUSKAL-WALLIS EQUALITY-OF-POPULATIONS RANK TEST: INT_EMPLOYEE.....	103
TABLE A.4.15. <i>PM</i> : KRUSKAL-WALLIS EQUALITY-OF-POPULATIONS RANK TEST: ORGANIZATIONAL SUBDIVISION.....	103
TABLE A.4.16. <i>PM</i> : LOGISTIC REGRESSION RESULTS. Y= PARTICIPANTS CLICKED THE EMBEDDED LINK (WITHOUT THE NVWA).....	104

TABLE A.4.17. <i>PM</i> : OVERVIEW WALD- χ^2 TEST RESULTS OF THE DIFFERENCES BETWEEN ORGANIZATIONAL UNITS OF THE NUMBER OF PARTICIPANTS WHO CLICKED ON THE EMBEDDED LINK IN THE PHISHING MAIL.	105
TABLE A.4.18. <i>PM</i> : OVERVIEW WALD- χ^2 TEST RESULTS OF THE DIFFERENCES BETWEEN AGE CATEGORIES OF THE NUMBER OF PARTICIPANTS WHO CLICKED ON THE EMBEDDED LINK IN THE PHISHING MAIL.	105
TABLE A.4.19. <i>PM</i> : FISCHER EXACT AND CHI2 TEST RESULTS – VISITING THE SITE : GENDER .	105
TABLE A.4.20. <i>PM</i> : FISCHER EXACT AND CHI2 TEST RESULTS – VISITING THE SITE : EMPLOYEE CONTRACT.....	105
TABLE A.4.21. <i>PM</i> : CORRELATION MATRIX PHISHING MAIL EXPERIMENT (Y=M2_VISITLINKBIN)	106
TABLE A.4.22. <i>PM</i> : VIF VALUES PHISHING MAIL EXPERIMENT	107
TABLE A.4.23. <i>PM</i> : LOGISTIC REGRESSION RESULTS. Y= PARTICIPANTS FILLED IN PASSWORD (WITHOUT THE NVWA).....	108
TABLE A.4.24. <i>PM</i> : OVERVIEW WALD-TEST χ^2 TEST RESULTS OF THE DIFFERENCES BETWEEN ORGANIZATIONS OF THE NUMBER OF PARTICIPANTS WHO FILLED IN PASSWORD.....	109
TABLE A.4.25. <i>PM</i> : OVERVIEW WALD χ^2 TEST RESULTS OF THE DIFFERENCES BETWEEN AGE CATEGORIES IN THE NUMBER OF PARTICIPANTS WHO FILLED IN PASSWORD.	109
TABLE A.4.27. <i>PM</i> : FISCHER EXACT AND CHI2 TEST RESULTS – VISITING THE SITE: EMPLOYEE CONTRACT.....	109
TABLE A.4.26. <i>PM</i> : FISCHER EXACT AND CHI2 TEST RESULTS – FILLED IN PASSWORD: GENDER	109
TABLE A.4.28. <i>PM</i> : CORRELATION MATRIX PHISHING MAIL EXPERIMENT	110
TABLE A.4.29. <i>PM</i> : VIF VALUES PHISHING MAIL EXPERIMENT	111
TABLE A.4.30. <i>SL</i> : AVERAGE PURE WORKING TIME, NUMBER OF OBSERVATIONS AND TOTAL PURE WORKING TIME DISAGGREGATED PER TREATMENT GROUP AND TIME PERIOD	112
TABLE A.4.31. <i>SL</i> : T-TEST RESULTS; NUMBER OF TIMES OF MANUALLY LOCKED SCREENS. THE INTERVENTION PERIOD, COMPARED TO THE SHORT-TERM POST-TEST AND LONG-TERM POST-TEST PERIOD, AND SHORT-TERM POST-TEST AND LONG-TERM POST-TEST COMPARISON, PER TREATMENT GROUP.	113
TABLE A.4.32. <i>SL</i> : T-TEST RESULTS, RATIO MANUAL LOCKS TO TOTAL LOCKS. THE INTERVENTION PERIOD, COMPARED TO THE SHORT-TERM POST-TEST AND LONG-TERM POST-TEST PERIOD, AND SHORT-TERM POST-TEST AND LONG-TERM POST-TEST COMPARISON, PER TREATMENT GROUP.	113
TABLE A.4.33. <i>SL</i> : HAUSMAN TEST RESULT OF THE MAIN MODEL (FIXED RANDOM, SIGMAMORE)	114
TABLE A.4.34. <i>SL</i> : CORRELATION MATRIX FOR THE VARIABLES OF THE MAIN MODEL.....	115
TABLE A.4.35. <i>SL</i> : VIF VALUES OF VARIABLES IN THE MAIN MODEL	116
TABLE A.4.36. <i>SL</i> : WOOLDRIDGE TEST FOR AUTOCORRELATION IN PANEL DATA: EXTENDED MODEL	117
TABLE A.4.37. <i>SL</i> : MODIFIED WALD TEST FOR GROUPWISE HETEOSKEDASTICITY: EXTENDED MODEL	117
TABLE A.4.38. <i>SL</i> : FIXED EFFECTS REGRESSION RESULTS. Y= NUMBER OF TIMES PARTICIPANTS MANUALLY LOCKED THEIR SCREEN.....	118
TABLE A.4.39. <i>SL</i> : TREATMENT IMPACT COMPARISON IN THE INTERVENTION PERIOD	119
TABLE A.4.40. <i>SL</i> : TREATMENT IMPACT COMPARISON IN THE SHORT-TERM POST-TEST PERIOD	119
TABLE A.4.41. <i>SL</i> : TREATMENT IMPACT COMPARISON IN THE LONG-TERM POST-TEST PERIOD.	119
TABLE A.4.42. <i>SL</i> : TREATMENT IMPACT COMPARISON OF PER2-PER3, PER2-PER4 AND PER3-PER4	119
TABLE A.4.43. <i>SL</i> : HAUSMAN TEST RESULT OF THE EXTENDED MODEL (FIXED RANDOM, SIGMAMORE)	120
TABLE A.4.44. <i>SL</i> : CORRELATION MATRIX FOR THE VARIABLES OF THE MAIN MODEL.....	121
TABLE A.4.45. <i>SL</i> : VIF VALUES OF VARIABLES OF THE EXTENDED MODEL (1/2).....	124

TABLE A.4.46. <i>SL</i> : WOOLDRIDGE TEST FOR AUTOCORRELATION IN PANEL DATA: EXTENDED MODEL	125
TABLE A.4.47. <i>SL</i> : MODIFIED WALD TEST FOR GROUPWISE HETEOSKEDASTICITY: EXTENDED MODEL	125
TABLE A.4.48. <i>SL</i> : FIXED EFFECTS REGRESSION RESULTS, WITH THE NUMBER OF TIMES PARTICIPANTS MANUALLY LOCKED THEIR SCREEN AS INDEPENDENT VARIABLE – EXTENDED MODEL	126
TABLE A.4.49. <i>SL</i> : TREATMENT IMPACT COMPARISON IN THE INTERVENTION PERIOD	127
TABLE A.4.50. <i>SL</i> : TREATMENT IMPACT COMPARISON IN THE SHORT-TERM POST-TEST PERIOD	127
TABLE A.4.51. <i>SL</i> : TREATMENT IMPACT COMPARISON IN THE LONG-TERM POST-TEST PERIOD	127
TABLE A.4.52. <i>SL</i> : TREATMENT IMPACT COMPARISON OF PER2-PER3, PER2-PER AND PER3-PER4	127

Figure overview

FIGURE 3.1. <i>SL</i> : SLOGAN INFORMATION CAMPAIGN	33
FIGURE 3.2. <i>SL</i> : STICKER TREATMENT CONDITION - (CONSTANT) SALIENT REMINDERS.....	33
FIGURE 4.1. <i>PM</i> : PARTICIPANTS' AGE DISTRIBUTION BY GENDER.....	38
FIGURE 4.2. <i>PM</i> : PERCENTAGE OF PARTICIPANTS WHO VISITED THE SITE PER TREATMENT (* SIGNIFICANTLY DIFFERENT COMPARED TO THE CONTROL GROUP).	39
FIGURE 4.3. <i>PM</i> : PERCENTAGE OF PARTICIPANTS WHO FILLED IN THEIR PASSWORD PER TREATMENT (* SIGNIFICANTLY DIFFERENT COMPARED TO THE CONTROL GROUP).	39
FIGURE 4.4. <i>PM</i> : PERCENTAGE OF PARTICIPANTS WHO FILLED IN PASSWORD OF THOSE WHO CLICKED ON THE EMBEDDED LINK (* SIGNIFICANTLY DIFFERENT COMPARED TO THE CONTROL GROUP)	40
FIGURE 4.5. <i>PM</i> : VISIT THE SITE (T=0) , RESPONSES OVER TIME (SEND 09:00).....	46
FIGURE 4.6. <i>PM</i> : FILLED IN PASSWORD RESPONSES OVER TIME. (SEND 09:00).	46
FIGURE 4.7. <i>SL</i> : PERCENTAGE INCREASE OF MANUAL LOCKS PER HOUR WORKED, COMPARED TO THE PRE-TEST PERIOD.	48
FIGURE 4.8. <i>SL</i> : ABSOLUTE CHANGE OF MANUAL LOCKS PER HOUR WORKED, PER PERIOD.....	48
FIGURE 4.9. <i>SL</i> : PERCENTAGE INCREASE OF THE RATIO OF MANUAL LOCKS TO TOTAL LOCKS, COMPARED TO THE PRE-TEST PERIOD.	50
FIGURE 4.10. <i>SL</i> : ABSOLUTE CHANGE OF THE RATIO OF MANUAL LOCKS TO TOTAL LOCKS, PER PERIOD.	50

Chapter 1: Introduction

According to the annual Global State of Information Security Survey 2015 (PwC, CIO & CSO, 2015) detected security incidents increased with 48 percent in 2013. This total of 42,8 million detected incidents, 117.339 a day, is however just a fraction of the true number of cases, because it is estimated that approximately 71 percent of incidents go undetected. Since organizations heavily rely on information systems, it is therefore extremely important to counter, and if not possible, mitigate security incidents.

To cope with increased information security threats and ensure information security, organizations actively deploy technical security measures (Bada & Sasse, 2014). Although these protective mechanisms contribute to improved information security (Ransbotham & Mitra, 2009), relying on them entirely (or excessively) is rarely enough to protect against threats. While organizations invest more and more in technology based solutions, the number of incidents related to information security is still increasing (PwC, CIO & CSO, 2015).

Researchers including Pahnla et al. (2007) and Vroom and von Solms (2004) have indicated that organizations which take both technical as well as non-technical protective means to heart are likely to be more successful in protecting against information security risks. Thus, success in information security can be accomplished when organizations devote to both technical and socio-organizational resources (Bulgurcu, Cavusoglu & Benbasat, 2010). In fact, it has been reported that individuals often constitute the weakest link in information security (Warkentin & Willison, 2009). Increasingly, attention in the literature is therefore being focused on socio-organizational resources, such as; policies, procedures, organizational culture, and the role individuals play in security (Herath & Rao, 2009). Organizations create such policies and procedures, to assist employees to ensure information security, while they utilize information systems in the course of performing their jobs (Whitman & Mattord, 2003). Although constructing policies and procedures is an essential outset, it is not enough to make sure employees' comply with them. Even if employees are fully aware of existing policies, computer-users may choose not to comply, when experiencing a trade-off between information security protection, and daily tasks (Ifinedo, 2011). Therefore, a better understanding of what factors motivate employees' compliance can help achieving more information secure behaviour.

Furthermore, vulnerabilities of the human factor in information security are also ascribed to non-intentional behaviour. Although users are motivated to perform information secure behaviour, some may simply lack knowledge, skills and abilities to protect themselves against posed threats, and to comply with existing policies (Albrechtsen, 2007). Internally, organizations broaden the tasks of key executives and Board of Directors to allow for improved communication of information security threat information and aid developing better-prepared, more resilient information security capabilities (PWC, CIO & CSO, 2016). Moreover, to cope with the problem, they implement most commonly used approaches of information security education, awareness and training (Siponen, 2006). This helps educating employees and executives about essential information security topics and human vulnerabilities.

Extensive literature, acknowledge to some (in)direct extent the importance of Security Education Training and Awareness (SETA) programs as an immediate and important predictor of changes in behaviour (Dhillon, 1999; Warkentin, Carter, & McBride, 2012; Whitman, 2004; Siponen, 2000; Waly, Tassabehji, & Kamala, 2012). Its main purpose of SETA programs is to increase employees' awareness and knowledge of potential security risks, policies and responsibilities. In terms of influencing individual employee behaviour, it is believed that user training and awareness of the risks to information security is a prerequisite factor that leads employees to comply with information security policy. (Lee & lee, 2002; Straub & Welke, 1998; D'arcy et al., 2009). Furthermore Warkentin et al. (2012) states that training is usually utilized as a primary mean to provide end-users with the necessary skills to influence behaviour.

1.1 The research question

This thesis aims to analyse the human factor in information security. Based on two field experiments; phishing and screen locking; we propose and test several interventions to improve information secure behaviour.

A first step is to analyse "why" individuals engage in information (in) secure behaviour. As mentioned, it could be non-compliance with security policies, such as leaving your screen unlocked and unprotected, or due to lack of skills and knowledge, when computer end-users are not able to distinguish between genuine and fraudulent mails. Many more determinants of the "why" can be mentioned, as will be discussed in the next chapter.

Second, we translate the why question to, "what" can we do about it. Although technological protective measurements are essential and can still be improved, we will limit this thesis to "what" impact security education, training and awareness programs (can) have on information (in)secure behaviour. More specifically, which specific elements of training can improve information (in)secure behaviour?

Third, we test "how" effective security education, training and awareness programs are in changing behaviour and "which" elements are more/or less effective in enhancing and improving information secure behaviour. As stated, we focus this thesis on; (1) phishing emails, and (2) screen locking. In two experiments we tested the impact of (1) information provisions, (2) (personal) experience, and (3) constant salient reminders on information secure behaviour.

In the end, we hope this can give us answer to the following thesis question;

How can information secure behaviour be effectively promoted in an organizational context?

In the remainder of this chapter we will give some background on topics of phishing and screen locking procedures and a short introduction to the setup of our field experiments. Furthermore, we describe the scientific and practical relevance of our study and end this section with the outline of the remainder of this thesis.

1.1.1 Phishing

The term phishing refers to an attempt to deceptively acquire personal and/or financial information (usernames, passwords etc.) by electronic communication with malicious intent (Ramanathan & Wechsler, 2013). Phishing is most commonly done via email, but occasionally, other (newer) methods of communication, like social networking websites, are being used. The text of a phishing mail, mostly, addresses the recipient with urgency cues, words that invoke feelings of vulnerability or threat, in order to try to force the recipient to act immediately and impulsively. These urgency cues are most deceitful, because they turn attention away from other cues that may potentially help the receiver to recognize a phishing mail (Vishwanath et al., 2011). Attackers can also trick users into downloading malicious malware, after they click on a link embedded in the email (Ramanathan & Wechsler, 2013).

Nowadays phishing mails have evolved from poor designed -and general phishing mails, into personalized -and well -designed phishing mails. These new emails, spear phishing attacks, are more dangerous because phishers use previously obtained personal information to make the phishing email appear more personal, hence increasing the chance of trustworthiness of the recipient. They make use of identity linking and victim selection, which results in the recipient to be more likely to believe the message is expected and legitimate (Blythe et al, 2011; Berghel, 2006). Although technical solutions such as spam filters, virus scanners, browser software, it-professionals etc. already temper the largest fraction of this threat, the individual end-user still remains the last critical line of defence, as a mail yet unexpectedly eludes these technical measures.

1.1.2 Screen locking

Screen locking refers to the security procedure most organizations impose, to protect sensitive and important data. Employees are required to always lock their screen, when they leave their workstation, regardless of the duration of absence. Otherwise, when leaving your workstation unlocked, anyone can use it and assume your network identity, gaining access to any applications or files to which you have access to.

As technical solution, computers in most organizations are automatically locked after fifteen minutes of inactivity. However, in this timeframe malicious intenders may already have struck. Therefore it is the computer end-user who can ensure someone does not get the opportunity to do so.

1.2 Field experiments

In the first experiment, we tested if information provision and/or providing a personal experience can lower the likelihood that an employee becomes victim of phishing fraud. In a time frame of 6 weeks, half of the employees of the Dutch Ministry of Economic Affairs received three informative emails regarding the topic phishing. Others received a phishing mail in advance to familiarize participants with phishing fraud. Both interventions taught people about phishing during their normal use of email, and were developed to increase awareness and knowledge of the recognition and reporting of phishing. Employees were unaware to be part of an experiment.

In the second experiment, screen locking (e.g. manually locking your screen), we tried to increase information security policy compliance of not leaving your screen unprotected and unlocked. Therefore we tested the impact of information provision and/or constant salient reminders on the number of times participants manually locked their screen. To emphasize desired behaviour, participants in the constant salient reminder treatment received green stickers on the keyboard shortcut, by which they could simply manually lock their screen. After, we established the baseline of each group in a pre-test, we tested for two weeks, the impact of treatments in the intervention period. Furthermore we tested whether treatment effects remained, two weeks and two months after treatments were stopped. The structure of phishing and screen locking experiments will be elaborated in section 3.

1.3 The contribution of this thesis

1.3.1 Practical relevance

As in most large companies information security plays a role in all processes, which mainly depends on human behaviour in addition to technical protective measures. Therefore in 2014, the ministry of Economic Affairs launched a government-wide campaign regarding information security, called iBewustzijn. It was aimed at helping employees and managers to improve digital skills and to help recognize- and prevent security risks. As part of the campaign e-learning courses and educational materials (e.g. posters, flyers etc.) were freely available. However results indicated that only a very small group of employees had made use of these online courses and educational materials.

This study therefore contributes to the government wide campaign regarding information security, by testing possible interventions and its effectiveness. Furthermore overall, it increases the awareness of employees, as noticed afterwards. Besides that this study can reveal efficient intervention strategies, it also can identify target groups of higher/lower risk. Those at highest risks could therefore be extra guided by IT professionals, for instance by giving extra training. This could both increase effectiveness of trainings as decrease expenditures. Furthermore, the phishing mail experiment can serve as a fire drill, to observe how employees, IT professionals, management etc. would respond to the mail and 'imposed threat'.

1.3.2 Scientific relevance

Furthermore the thesis contributes to the existing but still growing body of evidence of which specific elements of training are effective in promoting information secure behaviour. Since education, training and awareness programs are very divers, this study give support for which specific elements does or does not have impact on promoting information secure behaviour. To our best knowledge no study so far, have studied the topic screen locking policy compliance improvements. Although studies have indicated the effectiveness of (constant) salient reminders on behavioural change, we expand this scope by relating it to information security. Besides testing effectiveness of interventions, this study also describes the determinants of non-compliance and information secure behaviour.

Moreover, although existing studies have examined the impact of training and education on susceptibility to phishing fraud, few did so in an organizational context. Most studies involved role-

play activities or an university setting, of which results could be different, due to population and-or observer-expectancy bias. In this study we have tested effectiveness of interventions with complete waiver of consent, in a large scale experiment. Therefore, we were able to approach the situation of a received phishing email as realistic as possible, allowing us to observe actual behaviour which was not affected by experimental biases. It therefore complements prior studies with respect to phishing mail interventions, but tries to contribute by doing so in an organizational context. Besides testing the effectiveness of interventions, we tested whether gender, age, employee contract and differences between organizational division, affected susceptibility to phishing fraud.

1.4 Structure

The remainder of this thesis is structured as follows. In *chapter 2*, we give an in literature overview of what factors drive individuals to perform information (in)secure behaviour. Furthermore we discuss existing literature related to security education, training and awareness programs and its implications for our study and interventions. By reviewing existing literature, we end this chapter with the formulation of research questions and hypothesis. *Chapter 3* describes the research methods used in this thesis, such as; group formations and step-by-step procedure of the experiments. In *chapter 4*, we present how and what we have measured in these field experiments and the results of the experiments, statistical tests and regression analysis. Additionally some extra findings are presented. *Chapter 5* starts with a small recap of main findings, which we discuss in relation to the proposed research questions and hypothesis. Also, we propose the implications of our findings and some limitations of this thesis, and directions for future research. Finally, concluding remarks are presented in *chapter 6*.

Chapter 2: Literature overview

As mentioned in the introduction, information security is a very broad concept. Some elements involve high risk (phishing, viruses, malware), some lower risk (screen locking); it could occur in the (private) home setting, or in organizations; behaviour could be habitual/ frequently (screen locking) or infrequent (phishing); it could involve malicious behaviour, or non-intended; etc..

With so many factors included it goes without saying that there is not a 'holy information-security-bible' with all the answers on how one could transform information insecure behaviour into secure behaviour. Therefore, in this section we will try to get more insight in two important questions, namely;

- (1) What do we know about why, when & which people do (not) perform information secure behaviour (i.e. do (not) comply with information security policies (ISP's)), and;
- (2) What do we know about possible trainings / educational materials on how to increase information secure behaviour (i.e. increase compliance to information security policies (ISP's)).

The outline of this section is as follows. At first, in order to answer the first question, we will discuss the determinants of information (in)secure behaviour. What causes people to behave (in)securely and why do some people behave more secure than others? Furthermore, we will give some general insights into Security Education, Training and Awareness (SETA) programs, developed to promote secure behaviour. Moreover, we will discuss previous findings about "what works". Which interventions could contribute to more secure behaviour and what has been studied before? Finally we will propose our research questions and hypotheses.

2.1 Determinants of information (in)secure behaviour

"The greatest information security problem – the weakest link – is between the keyboard and the chair" (Warkentin & Willison, 2009).

Much has been studied on why, when & which people, do (not) perform information secure behaviour (Herath & Rao, 2009; Chan, Woon, & Kankanhalli, 2005; Pahnla, Siponen, & Mahmood, 2007; Siponen, Pahnla, & Mahmood, 2006; Zhang, Reithel, & Li, 2009; Ifinedo, 2011; Post & Kagan, 2007; Albrechtsen, 2007; Cheng, Li, Li, Holm, & Zhai, 2013). To fully address this question we will discuss the relevant antecedent factors for information (in)secure behaviour regarding clear-desk-clear-screen and phishing. Since both topics are affected by (some) different factors we will start by discussing determinants related to the topic of (manually) locking your screen.

2.1.1 Screen locking

"The main problem regarding users' role in the information security work is ascribable to their lack of motivation and knowledge regarding information security and related work."
(Albrechtsen & Hovden, 2010).

The most prominent factors for non-compliance regarding screen locking policies are low perceived risk and effort. According to the Protection Motivation Theory (PMT), (the intention of) (mal)adaptive response is a result of the appraisal of the threat- and coping response (Rogers, 1983). Since, many employees are simply unaware of how to perform specific protective countermeasures, the effort of doing so, is perceived higher than the opposed threat, resulting in low protective behaviour. Both risk communication and knowledge of how to perform protective behaviour could therefore contribute to more protective behaviour. Finally, individuals' behaviour is highly influenced by what others think and do. It could either encourage or- negatively affect, protective behaviour. In the following subsections, we will discuss the most relevant factors affecting a person's compliance to screen locking procedures.

Low perceived risk

If computer users perceive that a security threat can impose significant damages or disturbances, they are more likely to be concerned. Contrary, if they do not see that they are truly confronted by information security (IS) threats, they will have a less positive attitude towards protective behaviour. Both lines of reasoning are heavily supported in literature (Herath & Rao, 2009; Chan et al., 2005; Pahnla et al., 2007; Siponen et al., 2006;), of which the last, applies to screen locking behaviour.

There are two major reasons for the low perceived risk regarding screen locking behaviour. At first, computer users, especially in an organizational context, are protected by both physical and technical protection mechanisms (i.e. Entrance control, Detection systems, Guards etc.). According to the Compensation Theory (Adams, 1999; Adams, 1983), people take less cautious behaviour if they feel more protected. Although protective devices can help improve safety, they also encourage people to engage in more risky behaviour. This negative direct effect (i.e. perceived high technical and physical protection) leads to low intention to comply with organizational security policies. Empirically support for this statement was, inter alia, given by (Zhang et al., 2009). They found that perceived security protection mechanism is negatively related to end-users' intention to comply with security policy.

Secondly, According to the Protection Motivation theory, both the vulnerability and the severity of the threat affect ones risk perception (Rogers, 1983). Since little is known about the negative effects of leaving your screen unlocked, less emphasize is placed upon the threat. If locking your screen is so important, why are large information security campaigns mostly discussing threats such as phishing, viruses and malware, and almost never, the dangers of unprotected screens? Furthermore, why should you not trust your colleagues with an unlocked screen, since hardly anybody has (semi-) personal experience, with the negative consequences of leaving their screen unprotected? In short, individuals low risk perceptions are enhanced since they observe no consequences of leaving your screen unlocked.

Effort & hindrance with daily tasks

In day-to-day work, computer users may experience a trade-off between information security protection, and daily tasks (Herath & Rao, 2009; Ifinedo, 2011; Post & Kagan, 2007). In goal conflicts between acceptable risk and functionality, individuals tend to put emphasis on efficient and least-effort work instead of loss prevention (Albrechtsen, 2007). Therefore, employees are more likely to bypass security measures in order to complete a task, without hindrance in their normal routine (Post & Kagan, 2007). "Pressure from economic efficiency, the human desire for the least effort and security work creates migrating human behaviour within the space of boundaries of economic failures, unacceptable workload and unacceptable risks" (Albrechtsen, 2007).

Lack of knowledge

As mentioned, generates the combination of low perceived risk and 'hindrance' (in action and/or time) to daily tasks a less positive attitude towards protective behaviour. However Choi (2013) propose that perceived hindrance and effort is enhanced due to lack of computer-users knowledge (i.e. lack of self-efficacy of how to perform protective countermeasures). Locking your screen has been mentioned by end-users to be an unnecessary but mostly annoying task. However, just few are aware of the ease by which this protective measure could be performed (Auditdienst Rijk, 2014). Lack of knowledge therefore is not that individuals do not know *that* they should not leave your screen unprotected, but *how* a perceived "time consuming and annoying" task could be easily performed. Providing knowledge of easy to perform information security protective measures could therefore lower the hindrance- and effort trade-off with daily tasks (Choi, 2013).

Social influence

Another important element in explaining security compliance behaviour is social influence. Employees' perception of their peers and superior's complying with security policies has empirically shown to be significant predictors of employee intentions to comply with the policies themselves (Pahnila et al., 2007). Whereas normative beliefs have a significant impact on employees' behaviour, organizational culture is of high importance as a driving factor for the intention to comply with ISP' (Herath & Rao, 2009). Intentions are also driven by; shared beliefs, relationships between employees and perceptions of the organizational information security policies, practices and procedures. Therefore employees' behaviour is influenced by what relevant others do and by how they expect other colleagues to behave. (Aurigemma & Panko, 2012).

The effect of social influence on information secure behaviour could be two-sided. On the one hand, if the influence of peers and superiors is positively related towards information secure behaviour, this could encourage others to also behave according ISP (Van Niekerk & Von Solms, 2006). However if it is more or less generally accepted to not lock your screen when leaving the workstation, it is more likely that others will see less reason to lock their screen. This could result in a negative attitude towards IT secure behaviour. Social influence perceptions can potentially be altered by management actions that promote good information practices through clear direction, and knowledge of what is necessary for managing information security risks (Van Niekerk & VonSolms, 2010).

Finally, contrary to the social influence principles, compliance to information security policies could also be seen as suspiciousness towards peers and superiors, and therefore undesired. This principle of social etiquette could result in less compliance with ISP. In line with the compensation theory, due to the physical and technical countermeasures in place, it could be seen that employees do not perceive other colleagues as a threat, what enhances the feeling of having nothing to hide (Cheng, Li, Li, Holm, & Zhai, 2013). Locking your screen, in a controlled environment, therefore could be seen as unwanted suspiciousness towards others.

Concluding, the most prominent antecedent factors for non-compliance regarding clear-desk-clear-screen, are; (1) low perceived risk, (2) effort and hindrance with daily tasks, (3) lack of knowledge, and (4) social influence. Security Education, Training and Awareness programs therefore could contribute to more protective behaviour; (1) by altering risk perceptions (communicate associated risks and consequences of unsafe behaviour), (2) by increasing end-users knowledge/ self-efficacy, and by showing that information secure behaviour is compatible with daily tasks, and (3) by influencing organizational culture through clearly stating policies and responsibilities of computer users and managers.

2.1.2 Phishing emails

"In other words, the influence of cognitive and information processing activities on phishing susceptibility are tempered by the individuals levels of motivation, their personality based beliefs, their prior knowledge, and their day-to-day experiences." (Vishwanath, Herath, Chen, Wang, & Rao, 2011)

A primary explanation of susceptibility to phishing is driven by the amount of attention paid to incoming emails. Furthermore, users lack knowledge of- and experience with the recognition- and reporting of phishing fraud. Moreover they distribute responsibility of detecting phishing to others, thereby lowering one self's risk perception. Finally users susceptibility is influenced by demographic and some other factors. In the following subsections, we will discuss the most relevant factors affecting a person's susceptibility towards phishing fraud.

Limited attention

Because the assessment of the genuineness of incoming emails is not a primary concern for individuals, computer end-users must often make quick decisions, based on cues found in the emails. However, faced with cues that require an immediate action and high work- and email load, this may disturb the ability to detect deception. Research conducted by Vishwanath et al. (2011) illustrated that attention paid to incoming emails is affected by; (1) workload, (2) knowledge, (3) computer self-efficacy, and (4) perceived relevance of particular messages. The level of attention to emails is negatively related to individuals' likelihood to respond to phishing emails.

Furthermore, coupled with high email load, users who reported to habitual social media use are more likely to automatically respond to relevant looking emails, thus increasing the likelihood of response to phishing emails. Vishwanath et al. (2011) found that technological self-efficacy and prior experience have no significant effect on phishing susceptibility. This implies that susceptibility to phishing fraud is not driven by lack of ability, but due to the lack of cognitive involvement (Viswanath et al., 2011). Moreover (Greitzer et al., 2014) found that due to workload users will take less time to view an email, hereby possibly missing cues about the authenticity of the email.

Lack of knowledge & Experience

Contrary to the findings of Viswanath et al. (2011), Wright & Marett (2010) and Downs, Holbrook, & Cranor (2007) found technological self-efficacy and prior experience with phishing emails to be negatively related to phishing fraud susceptibility. However they also found knowledge of phishing fraud to be often inaccurate and outdated. Although most users have heard the term phishing and are aware of the risks involved such as malware, they are unaware of the advanced and newer techniques of phishing fraud such as spear (context aware) and social engineering phishing attacks (Parsons, McCormac, Pattinson, Butavicius, & Jerram, 2013; Downs, Holbrook, & Cranor, 2007). In assessing a (in)genuine email users should focus their attention on elements which help you to identify phishing fraud, such as; (1) grammar and spelling, (2) urgency cues, (3) title/subject line and (4) email source (Viswanath et al., 2011). By placing more emphasis on these elements, this will ensure that recognizable cues of phishing fraud are less likely to be overlooked.

Another vital element is that users are most often unaware of information security policy guidelines. Even if they do recognize an email as being fraudulent, they could be unaware of how to report this email. As a consequence, if fraudulent emails are not being reported, this will limit the functionality of IT professionals, since they are not able to; (1) adjust spam filters, (2) test whether the fraudulent email has harmed the IT facilities, and (3) warn other computer users in the company. A prerequisite factor is that proper guidelines are established, communicated to personnel and updated, since unclear protocols and guidelines have reported to have a negative effect on increased susceptibility (Hu, Dinev, Hart, & Cooke, 2012)). Also, due to their exemplary role and supportive function, it is important that superiors are fully aware of existing guidelines and policies.

Distributed responsibility & low risk perception

In large companies, employees distribute the responsibility of information security to professionals in a certain amount. Due to high standard countermeasures (firewalls, virus scanners etc.) and IT professional assistance (technical support, customer service etc.), they overlook their personal role (Albrechtsen, 2007). By distributing responsibilities, people underestimate the risk involved with phishing fraud (and their personal role in it) (Zhang et al., 2009). Furthermore they underestimate the amount of (personal) information that malicious attackers can find on the internet. For example they underestimate the probability of work-email addresses to be known (Auditdienst Rijk, 2014). Due to the lack of personal- and others' experiences, individuals low risk perceptions are enhanced since they observe no consequences, distribute responsibility and underestimate the amount of (personal) information that could be known by fraudsters. An adverse unwanted effect is, that this reduces the amount of attention paid to incoming mails.

Demographic factors

Demographic factors have extensively been topic of research. A research conducted by Dhamija, Tygar, & Hearst (2006) found no significant correlation between education, age, sex, previous experience, hours of computer usage and susceptibility to phishing. However Jagatic, Johnson, & Menczer (2007) found that females are more likely to fall for spear phishing attacks, then males. This finding is supported by research by Sheng et al. (2007) and Kumaraguru et al. (2007). Both studies found, that men were more likely to correctly distinguish between phishing and genuine mails. However, in another study, Kumaraguru et al. (2009) did not found significant differences between males and females regarding susceptibility towards phishing fraud. They did however found that people aged 18-25, are more vulnerable to phishing attacks. This effect has also been supported by Sheng et al. (2010), who found that participants aged 18-25 were more likely than others to fall for phishing. As reasoning they propose that those have; (1) a lower level of education, (2) fewer years on the internet, (3) less (financial) risk aversion, and (4) less exposure to training materials.

Furthermore, targets are four times more likely to become victim of a phishing attack, if they are solicited by someone appearing to be an acquaintance. The social content of the attacks may lead people to overlook important cues, lowering the guard and thereby making themselves more vulnerable to phishing attacks (Jagatic et al., 2007). Moreover, victims are also more likely to fall for a phishing scam if the sender is of the opposite sex (Sheng et al., 2010). Other factors that are of relevance for the detection rate of phishing emails, are; (1) the visual presentation of emails (i.e. logos, banners etc.) (2) grammatical errors, (3) personalization of the email, (4) perceived legitimacy of the URL, (5) the sender (email address), (6) workload / stress , and (7) the tone of the email (urgency cues/ threats/ potential loss, which can cause an emotional response, making individuals act in a less rational manner)(Furnell, 2007; Parsons & McCormac, 2015; Blythe, Petrie, & Clark, 2011; Vishwanath et al, 2011).

To sum up, susceptibility to phishing fraud can be explained by; (1) lack of knowledge and experience; (2) poor security risk communication and proper guidelines, (3) expectancy of the employees that information security is a technological discipline handled by IT professionals, (4) limited attention paid to incoming mails (i.e. a latent conflict of interest between information security and daily work), and (5) demographic and other mentioned factors. The main problem regarding users' role in the information security environment is therefore merely their lack of motivation and knowledge (Besnard & Arief, 2004; Albrechtsen & Hovden, 2009).

2.2 Training Employees – The effect of Information, (Personal) Experience and Reminders

To counter information insecure behaviour, Security Education, Training and Awareness (SETA) programs are developed based on specific determinants that influence this (habitual) behaviour. The basis of current findings of proven effective measures is established in the health (economics) domain. In this domain, the impact of prevention, deterrence and education on (changes in behaviour) have been studied. The remainder of this chapter will focus on what already is known of interventions what (can) promote (information) secure behaviour. We will discuss interventions that have been proven to be effective in achieving this goal. For example, most of the literature focuses on trainings. However, the literature finds mixed effects for the effectiveness of trainings. One possible explanation is, that trainings are very divers (mass-media, information, videos, leaflets etc.) which makes it difficult to compare and pinpoint the effective elements. Another difficulty arises due to different types of information (in)secure behaviour. Whereas phishing is considered an infrequent and high risk threat, compliance to screen locking procedures is a more frequent and habitual behaviour, associated with lower (perceived) risks.

2.2.1 Security education, training and awareness programs (SETA)

"Consequently, security training was and continues to be one of the most important fundamentals to information security practices." (Puhakainen & Siponen, 2010)

Extensive literature, acknowledges to some (in)direct extent the importance of Security Education Training and Awareness (SETA) programs as an immediate and important predictor of changes in (intentions of) behaviour (Dhillon, 1999; Warkentin, Carter, & McBride, 2012; Whitman, 2004; Siponen, 2000; Waly, Tassabehji, & Kamala, 2012). The main purpose of SETA programs is to increase employees' awareness and knowledge of potential security risks, policies and responsibilities. In terms of influencing individual employee behaviour, user training and awareness of the risks to information security is considered a prerequisite factor that leads employees to comply with information security policy. (Lee & Lee, 2002; Straub & Welke, 1998; D'arcy et al., 2009). Furthermore Warkentin et al. (2012) state that training is usually utilized as a primary means to provide end-users with the necessary skills to influence behaviour.

Security Education Training and Awareness programs are available in a wide range of options, such as the distribution of messages via, e.g. mass media (Campaigns), videos, newsletters, posters, security web site and web ads, computer based training, online quizzes, case studies/ seminars/ discussion sessions, e-mails, intranet pages and screen savers (Albrechtsen & Hovden, 2010; Payne, 2003). In this thesis however we will limit our focus on how; (1) information provision, (2) learning by experience and (3) (constant) salient renders, can affect (in) secure human behaviour. Findings related to information provision are taken into account by developing interventions for both improving compliance with procedures of locking your screen, as reducing the likelihood of becoming victim of phishing fraud. Furthermore, findings related to learning by experience are applied in our phishing email field experiment, and findings of saliency and reminders in our screen locking experiment.

2.2.2 The effect of Information Provision

"...individuals will be more capable of making important decisions about precautionary and risk behaviors if they are more knowledgeable about the consequences of those behaviors".

(Gerrard, Gibbons, & Reis-Bergan, 1998)

"Fear appears to be a great motivator as long as individuals believe they are able to protect themselves." (Witte & Allen, 2000)

Risk communication is one of the most used strategic tools of improving information secure behaviour through information provision. Furthermore information provision has been applied to increase self-efficacy in order to allow users to gain know-how to (easily) perform protective measures. The possible improvement of self-efficacy, is however largely dependent of what- and how information is being communicated and processed. To increase effectiveness it is therefore recommended to incorporate social norms, and pay attention to the style and visual presentation of the communication strategy. In the following subsections, we will discuss the most relevant factors affecting the impact of information provision in order to improve information secure behaviour.

Communicating risk

One way of how information secure behaviour can be promoted is to properly communicate risks associated with particular behaviour. Theoretically for example, according to Protection Motivation Theory (PMT) and the Precaution Adoption Process Model (PAPM) (Weinstein & Sandman, 2002), risk communication can alter risk perceptions. The Precaution Adoption Process Model attempts to explain how a person comes to a decision to take action, and how this decision is translated into action. During six stages of this process, a person could be influenced by information, resulting in changes in precautionary behaviour. However this depends on, if severity and vulnerability of the risks is properly addressed, and if it includes the efficacy of the desired behaviour change. Also the effectiveness depends on how- and which information is presented, and how (due to individual differences) information is being processed (Gerrard et al., 1998; PMT & Fear Appeals: Rogers, 1983). However, there is still limited evidence supporting the promises that providing risk information is an effective tool to change risk perceptions, and even less evidence that altering risk perceptions motivates new secure behaviour.

In the health domain, much attention has been paid to how the level of knowledge assists in altering risk perceptions, and in turn protective behaviour. Providing users with more information about threats and consequences can increase their perceptions of susceptibility (Davison & Sillence, 2010). Witte & Allen (2000) indicate that the use of fear-arousal did have an effect on behaviour change. However, as also acknowledged by Davison & Sillence (2010), once a user is motivated via increased susceptibility, the user also needs to be aware of an effective coping strategy to prevent the occurrence of maladaptive responses. Thereby suggesting that, strong fear appeals and high-efficacy messages produce the greatest behaviour change (Davison & Sillence, 2010; Witte & Allen, 2000). In the phishing domain this implies to, having the knowledge and means to be able to detect- and report fraudulent messages. Findings of Davison & Sillence (2010) and Witte & Allen (2000) therefore conflict with previous research (Leventhal et al., 1997),

suggesting that interventions which simply inform people they are susceptible to risks, are not sufficient to change behaviour.

A research conducted by Kumaraguru et al. (2007) tested the effect of sending security notices to reduce susceptibility to phishing fraud. Their findings were in line with findings of Davison & Silence (2010) and (Sheng et al., 2007), since they found no significant differences in phishing susceptibility between the control group and the group who received security notices. One proposed explanation is limited attention towards security notices, due to its low perceived relevance. As information security is often not individuals primary concern, sending out information emails are often ignored (Mohebzada et al., 2012). In order to increase the likelihood that individuals actually would read the information they have been send, it is therefore important to incorporate urgency cues and make the message more visually salient (Ifinedo, 2011; Post & Kagan, 2007).

Self-efficacy

As mentioned in the previous section, Witte & Allen (2000) and Davison and Sillence (2010) acknowledge that the use of fear arousal should be combined with an effective coping strategy. In other words, one should not only be presented with information about the presence of threats, but also how one could mitigate and preferably eliminate the threat. Therefore for communication to be effective, it should enhance self-efficacy. To do so, studies have discussed effective strategies companies use, aimed to help to protect employees. They have listed most common used information to include; (1) list of types of information that the organization will never ask, (2) description of appropriate steps for protection against phishing, and examples of the newest phishing techniques (for example; context aware phishing), and (3) useful links for the employees where they could obtain other relevant information such as; examples of phishing emails and information about how to report suspicious emails (Baker et al., 2007; Parsons & McCormac, 2015; Kumaraguru et al., 2007).

Furthermore, also Sheng et al. (2010) proposed that training programs could be used to improve self-efficacy. They tested four experimental conditions, in which participants were shown educational material (cartoon, interactive role-play game, web-based training materials and a combination of the cartoon and role-play game). They found all of the educational materials to be effective in reducing the likelihood that participants entered information into phishing webpages by approximately 40%. However, participants who received web-based training materials also clicked significantly less on legitimate websites. This may suggest that those participants generated an avoidance strategy rather than a strategy for better detection.

To make sure a detection strategy rather than avoidance strategy is developed, Burns, Durcikova, & Jenkins (2013) propose stage-interventions. Participants in stage one were given information of what phishing is and what you can do to prevent becoming a victim of phishing. In the second stage, participants were given additional information about why- and how you should report a phishing email. Both interventions reported to be effective in reducing the likelihood of falling for phishing emails.

Moreover, according to Kumaraguru et al. (2007) & Ferguson (2005) the best training system is an embedded training system, one that both provides warnings as well as actionable items. Kumaraguru et al. (2007) and Sheng et al. (2007) also presented, based on other studies, design principles, that could be applied to the design of training messages and anti-phishing interventions; (1) make the participants clear what the risks are and what caused the warning, (2) keep the training messages simple and short, (3) provide clear actionable items that participants easily can adopt to protect themselves, (4) use story based graphics.

Social norms

Making use of social norms in communication has also been proved an effective communication tool (Berkowitz, 2005; Mehri & Midha, 2013). Users are influenced by what others do, and what they think that others do (Pahnila et al., 2007). Social norms theory predicts that revealing the actual norm to correct misperceptions will be beneficial for most individuals, who will either be encouraged to engage in protective behaviours or reduce their participation in potentially unsafe behaviour (Berkowitz, 2005). Although Venkatesh & Davis (2000) and Zhang et al. (2009) found that the use of social norms is effective in increasing information secure behaviour, this effect erodes with increasing experience. People who have been employed for many years tend to carry on their previous work practices, even if the opposite is expected by the social influence of peers and superiors (Berkowitz, 2005).

Style

Although content of trainings programs is of high importance, in order to be effective, attention should be paid to the style and visceral influences (Sheng et al., 2007). Research conducted by Kumaraguru et al. (2007) showed that simple cartoons increase the effect of educational material compared to standardized security notices. Furthermore, although Sheng et al. (2010) found that standard web-based trainings were effective in reducing the likelihood to enter information into phishing webpages, users in this condition also clicked less on legitimate links of websites. Participants who received the informative cartoon or played the interactive role play game however, were less likely to enter information on the phishing webpage (comparing to the control group) without the avoidance strategy of clicking less on the legitimate website links. The importance of (the combination of) text and images being simple and visually salient has also been acknowledged in research conducted by McCormac (2015).

To sum, as proposed by literature, communication could be effective to engage individuals into more protective and secure behaviour, although this is still largely dependent on how information is being communicated and processed. To increase effectiveness of informative security training materials, one should clearly; (1) communicate threats, (the why?) (2) describe the appropriate steps of prevention (coping strategy) (the how?), (3) incorporate social norms, and (4) list information companies would never ask, with taking into account; (1) keeping messages short and simple, (2) adding supportive images/ cartoons, and (3) to utilize the visual identity style of the target group.

2.2.3 The effect of (Personal) Experience & Feedback

"The results suggest that users can be trained using decoy technology to be cognizant of potential threats." (Bowen, Devarajan, & Stolfo, 2011)

Intervention studies in the information security domain have focused on the effectiveness of simulating previous experience on (in)secure behaviour. Both by role playing and decoy mails, the effect of simulated attacks on susceptibility to becoming a victim of phishing fraud has been tested. Effectiveness of such programs is enhanced by improved self-efficacy, feedback and learning-by-doing. In the following subsections, we will discuss the most relevant factors affecting the impact of simulating (personal) experience and providing feedback to improve information secure behaviour.

Personal experience generally leads people to see threats as more probable, present and to view themselves as potential future victims. As a consequence, interest in prevention is increased. Furthermore, due to social networks there is increased communication about potential threats and ways of reducing risk. Therefore they facilitate precautionary behaviour to the entire affected community, not just to those who have suffered individual harm (Smith & Tobin, 1979; Weinstein, 1989). However, the effect of individual experience on preventive behaviour is mitigated through; (1) modest experienced harm, (2) lack of confidence in precautions, and (3) the limited duration of impact (Weinstein, 1989).

Simulated phishing attacks

The effect of simulated attacks on susceptibility to phishing emails has been investigated by extensive studies (Downs et al., 2006; Wright & Marett, 2010; Bowen et al., 2011; Burns et al., 2013; Mohebzada, 2012). Whereas there are different explanations (learning-by-doing; altered risk perceptions; social influence) for the effectiveness of the positive relation between previous experience and phishing email susceptibility, all acknowledge to some extent the strength of using simulated phishing attacks as an effective intervention to lower phishing email susceptibility. At the American University of Sharjah (AUS) Mohebzada (2012) tested the effect of simulated attacks on susceptibility to phishing. He found that after sending a first decoy email, users who fell victim dropped from 17,90% (1.954/10.197) to 2,02% (220/10197) in the second round ($p < 0.001$). In a research conducted by Downs (2006), they found that familiarity with particular scams seems to be the best predictor for spotting similar ones. However, this benefit did not seem to extend to unfamiliar scams, what is most often the case in spear-phishing attacks.

Also Bowen et al. (2011) have tested a training technique by sending simulated phishing emails. Four groups (email with external URL, email with internal URL, forms to obtain credentials and email with possible fraudulent annex) of 500 students and faculty staff were send simulated phishing email attacks. Those who fall victim to phishing attacks were repeatedly send simulated phishing emails, and given feedback so that they may learn to change their behaviour. They found that generating experience with- and providing feedback about phishing emails, are effective in decreasing the likelihood of falling for fraudulent attacks.

Self-efficacy

According to Wright & Marett (2010) experiential factors are more influential to user's susceptibility and online deception than dispositional factors. They found that; (1) computer self-efficacy, (2) web experience, and (3) security knowledge are positively related to user's susceptibility ($p < 0,05$). Consequently, they propose that susceptibility to phishing could be reduced by well-established security programs, especially those that involve simulating experience with phishing emails.

Furthermore Siponen, Mahmood, & Pahnla (2014) & Ifinedo (2011) tested in a survey study the effect of self-efficacy and web experience on behavioural intentions. They reported self-efficacy and web experience to be significant predictors of users' behavioural intentions. In line with these findings, Ajzen (2012) and Taylor & Todd (1995) tested in a survey study the effect of self-efficacy on perceived behavioural control. These studies revealed self-efficacy to be significant predictors for perceived behavioural control. Both behavioural intentions and perceived behavioural control are grounded in the theoretical framework of the Theory of Planned Behaviour (TPB) and supported by empirical studies (Notani, 1998) to be driven factors of (change in) actual behaviour.

Learning by doing

Two major advantages of simulating phishing email attacks over general information provision are the *learning-by-doing* – and *feedback principles*. Research has shown that knowledge and skills are strengthened through practice (Burns et al., 2013; Bowen et al., 2011; Sheng et al., 2007). Furthermore this allows individuals to increase familiarization with phishing emails and to develop necessary skills in the recognition of phishing scam cues and- how to report it. Learning science suggests that simply telling people what to do is insufficient, "because it is better to present abstract information using concrete examples" (Kumaraguru et al., 2007). Sending fake phishing emails though, has been proven to be a good intervention to both test the user's vulnerability as to give additional information to teach participants about phishing attacks. Because these types of interventions provide the participants with clear actionable items, this will improve its effectiveness (Parsons & McCormac, 2015).

Feedback

The second principle, *feedback provision*, illustrates that feedback is advantageous in learning effectively, moving towards more correct behaviour, and engaging in less insecure behaviour (Kumaraguru et al., 2009). Direct feedback is preferred over delayed feedback, because it eliminates the gap between cause (clicking on a link) and effect (seeing warning messages about the phishing email) (Kumaraguru et al., 2007).

In a meta-analysis of 607 studies Kluger & DeNisi (1996) found that, in general, more than 60 percentage of all feedback interventions increased performance. Feedback supports reflection by increasing knowledge and awareness of behaviours and their impacts (Hermsen et al., 2016). Since many behaviours are of such automaticity, their performance also account for being partially subconscious. Therefore knowing that- and when a habit occurs enables us to analyse its consequences and to adapt if necessary (Alberts et al., 2011).

Embedded training

Best is, according (Bowen et al., 2011; Kumaraguru et al., 2007; Burns et al., 2013, Sheng et al., 2007), to incorporate the information provision and experience generation of phishing emails into one training material (embedded training). If individuals are given information after they have received a phishing email, this will increase the perceived relevance of the information. Whereas according to Sheng et al. (2007) training materials, in the form of solely information provision, merely only increases awareness about phishing (which could help people avoid phishing scams), an embedded training system makes users more knowledgeable about techniques they can use to identify phishing emails/sites.

To sum, due to the learning-by-doing- and feedback principle simulating phishing attacks has been a widely applied strategy to reduce susceptibility of phishing attacks. By simulating phishing attacks, users can generate skills necessary to recognize and report phishing emails. It is most effective when simulated attacks are accompanied by additional educational information.

2.2.4 The effect of emphasizing desired behaviour

"One of the most effective countermeasures for reducing errors of omission is the use of reminders." Furthermore, "errors of omission often can be reduced by increasing a target's salience, thereby drawing attention to it." (D'Egidio et al., 2014)

Studies, aimed at testing interventions based on reminders and saliency, have mostly been associated with habitual behaviour (for example, weekly gym attendance, to take medication and hand hygiene). They found that (constant) salient reminders can be effective in changing habitual behaviour, to the extent of generating new, long-lasting habitual behaviour. Effectiveness of reminders is influenced by how and when they are presented. Reminders are used to derive someone's attention to the desired options or behaviour. Attention in its turn could be enhanced by increasing the salience (i.e. visibility) of desired behaviour or options. In the following subsections, we will discuss the most relevant factors affecting the impact of emphasizing desired behaviour to improve information secure behaviour.

Reminders

A growing body of evidence shows that reminders (text-messages / emails) can have a substantial impact on behaviour. This has been studied in; (1) improved gym-attendance (Calzolari and Nardotto, 2011), (2) increased savings deposit (Karlan et al., 2010) and (3) health protective behaviour (Raifman et al., 2016; Maurer and Harris, 2014; Hasvold & Wootton, 2011). These results show that reminders are effective regardless of the nature of the underlying activity. One possible explanation is that a stimulus, such as a reminder, focuses the attention of the receiver towards the inflicted goal, and further away of many alternative goals. (Calzori & Nardotto, 2015). Taubinsky (2014) states that people are inattentive, and will not take actions which are not in mind. A basic implication of this is that cues (reminders) that direct people's attention to a particular action should make its execution more likely.

However, Taubinsky (2014) highlighted that reminders are imperfect. Although cues can have strong effect on behaviour, reminders (for example emails) do not always reach the individual. Furthermore, due to limited cognitive abilities, even within a time period of a day, the received reminder could just simply not be recalled at the time of 'need'. Moreover, an individual's attention, derived by the reminder, decays over time until another reminder is received. The once salient intentions, may no longer be desired, or reshaped through daily tasks and distractions, and new goals. Calzori & Nardotto (2015) studied the effect of relatively high frequency reminders on gym-attendance, and found lowered gym-attendance on days with no reminders compared to days were individuals where send reminders. This implies that reminders are more effective when they are sent shortly before the behaviour is to take place.

To counter above mentioned mitigated effectiveness of reminders, one could simply propose to increase the frequency of reminders (Demakis, et al., 2000). In a research conducted on web-based questionnaires, Svensson, Svensson, Hansen, & Lagerros (2012) found that the more reminders used, the higher the increase of response rate (3 groups; low-medium-high frequency reminders). However, if reminders are sent more frequently, they may result in being less effective, because users will pay less attention to them. On the other hand, more frequent reminders may have stronger effect if their capacity to increase attention quickly decays (Calzolari & Nardotto, 2015).

Furthermore some studies (Calzolari & Nardotto, 2015; Taubinsky, 2014; Zurovac, 2011) have analysed the long-lasting effect of reminders. Once reminders have increased a user's attendance for a considerable period of time, then for repeated actions – such as locking your screen –habit-forming behaviour may occur. The more a person has performed particular behaviour in the past, the more likely they are to be top of mind, and thus the more likely they are to be performed again (Taubinsky, 2014). Taubinsky (2014) and Zurovac (2011) both found that treatment effects, although diminished, remained upon 2 to 6 months after reminders had been stopped.

An important element in effectiveness of reminders is how they are presented to individuals, since reminders could vary from plain-text messages to the extreme of your beloved one saying to do the dishes. For example; (1) Hasvold & Wooton (2011) found that automated reminders were less effective than personal phone calls, (2) Karlan et al. (2010) showed that reminders that emphasized specific intentions, were two times more effective than reminders that did not mention it, (3) and Charles et al. (2007) stated that the combination of visual and audio reminders in an electronic pill bottle, increased the adherence of taking medicines.

In an experiment conducted by Lewis & Eves (2011), subjects were motivated through reminders to take the stairs instead of the elevator. They found no significant effect in number of participants taking the stairs, when the poster was placed in the elevator. However, the number of participants taking the stairs increased significantly, when the poster was replaced at the time and place of the decision making process of taking the stairs or to use the elevator. Meaning, that the visibility of a stimulus at the time the behavioural choice was made was necessary to change actual behaviour.

Saliency

Another proposed intervention to change habitual behaviour is; increasing the saliency of the desired behaviour. For example, D'Egidio et al., (2014) found that flashing lights increased the saliency of alcohol-gel dispensers and that this improved hand hygiene compliance in a hospital. They found that, a simple and inexpensive flashing red light to be sufficiently salient to more or less double overall hand hygiene compliance. The intervention drew attention to the alcohol dispensers, which in turn reminded employees to wash their hands. In a related study, Nevo et al. (2010) also focused on hand hygiene compliance. Tested interventions revealed that both the location of the alcohol dispenser (line-of-sight) and visual salient cues (warning sign & flashing lights) significantly improved hygiene compliance.

Furthermore Garner (2005) reviewed four studies that have examined the influence of attaching a seemingly insignificant post-it note to a survey packet on the likelihood of completing the survey. Using a visual salient reminder resulted in significantly higher return rates than participants who received the identical survey without the Post-It. In addition, personalization of the post-it enhanced these significantly higher return rates.

Finally, Just & Wansink (2009), Privitera & Creary (2013), Painter & Wansink (2002) and Wansink, Painter, & Lee (2006), all analysed the influence of visibility on making healthier choices. In a school in Minnesota, Just & Wansink (2009) found that students who waited to pay, were faced with a wide array of unhealthy food. By simply replacing these snacks with fruits, fruit sales increased, snack food sales decreased and total revenue did not significantly decrease. Wansink et al. (2006) tested the influence of visibility in an office setting. Employees significantly ate an average of 2,2 more candies each day when they were visible. These findings were also supported by Painter & Wansink (2002). Furthermore Privitera & Creary (2013) tested differences between placing fruit and vegetables in an opaque bowl versus a clear bowl, whereby visibility significantly increased consumption of apple slices but not carrot cuts.

To sum, as proposed by literature, saliency nudges, by increasing the visibility of a particular option or behaviour, may emphasize desired behaviour, resulting into more compliance. Another way habitual behaviour can be influenced, is by modifying the environment within which decisions are made. Such modifications may increase the saliency and attractiveness of a particular option or behaviour, making it more likely that it is selected or executed (Wilson et al., 2015). Furthermore, reminders could be effective in changing actual behaviour, even to the extent of generating habitual behaviour, by which the behavioural change remain, although reminders have been stopped. Effectiveness of reminders on behaviour however, is largely influenced by when, where and how reminders are presented to individuals.

2.3. Research question & Hypotheses

This thesis addresses, the effect of information security training on (in) secure behaviour, focusing specifically on; (1) phishing emails and (2) screen locking behaviour. In two experiments we test, whether; (1) information provision, (2) simulating (personal) experience and (3) (constant) salient reminders are effective in improving information secure behaviour. On the basis of these experiments and prior literature, we aim to answer the following questions;

Main Question: How can information secure behaviour be effectively promoted in an organizational context?

2.3.1 Phishing

Our first subject of experiment is phishing emails. To analyse the results of our experiment, we have determined two standards of measurement, which could be improved by our treatments. First we test the effect of our treatments on the number of participants that have visited the link enclosed in the email. Second, whether individuals had filled in personal details at our controlled 'fake' website(s). On the topic of phishing emails, we are interested in;

RQ1: What treatments are effective in reducing subjects' susceptibility to becoming a victim of phishing email fraud?

RQ2A: What demographic factors affect someone's' likelihood to fall for phishing email attacks?

RQ2B: How does the type of employment (external/ internal) contract affect susceptibility to phishing email fraud?

In our experiment we test three treatments to see which training elements are effective in reducing susceptibility to phishing emails; (1) information provision (three info graphics by mail), (2) simulating experience with phishing and (3) an embedded training, of both information provision and simulated experience with phishing emails (combined treatment). We propose;

H1A: Information provision is effective in reducing the likelihood of falling for phishing email fraud attacks.

H1B: Previous experience with phishing emails reduces the likelihood of falling for phishing emails.

H1C: An embedded training, of combined treatments, is most effective in reducing the likelihood of falling for phishing emails. The effect however is not synergetic in nature.

To answer our third research question, we test whether demographics factors influence the likelihood of becoming a victim of phishing email fraud. Based upon findings in literature, we propose;

H2A: Age is negatively related to increased susceptibility to phishing emails. This means that an increase in age decreases the likelihood of becoming victim of a phishing email attack.

H2B: Gender has no effect on susceptibility to phishing emails.

Finally, as social context and perceived relevance are important determinants affecting the likelihood that someone is deceived by a phishing email, we want to examine whether the type of employment contract affect susceptibility to phishing emails.

H2C: Employees with an external employee contract are less susceptible to phishing emails.

2.3.2 Screen locking

In our *second experiment* we monitored participants' behaviour regarding compliance with screen locking procedures. We have applied the following standard of measurement to analyse whether subjects follow information security policies, and lock their screen when leaving their workstation. An improvement in behaviour is achieved if the number of times participants manually locked their screen increases.

RQ3: What treatments are effective in improving screen locking behaviour?

RQ4: What treatments are long-lasting effective in improving screen locking behaviour?

RQ4: What is the effect of relative occupancy of workstations and number of hours worked on screen locking behaviour?

We have tested effectiveness of three treatments; (1) information provision (handing out information flyers), (2) constant salient reminders (keyboard shortcuts by which you can lock your screen are highlighted by green stickers), and (3) the combined treatment of both information provision and constant salient reminders. We hypothesize;

H3A: Information provision is effective in improving participants' screen locking behaviour.

H3B: Constant salient reminders improve participants' screen locking behaviour.

H3C: The combined treatment is most effective in improving participant' screen locking behaviour.

To analyse if treatments will lead to habit forming behaviour, we tested if treatment effects are long-lasting. After treatments were stopped, we continued measuring results for two months. We expect that participants, who are in the constant salient reminder groups, will retain improved behaviour, although (probably) diminished. Furthermore we expect to see no long-lasting effect in improved behaviour for participants who only received the information flyers.

H4: The constant salient reminder treatment effect is long-lasting (i.e. it will maintain improved behaviour), but the treatment effect of information provision is not (long-lasting).

Our next subject of interest is whether relative occupancy of workstation has an effect of clear-screen locking behaviour. In other words, we want to test the effect of the ratio of occupied workstations to the total of workstations per hallway, on screen locking behaviour. Extensive literature has acknowledged the social influence principle of peer and superiors (and social control), so we expect a relative high occupancy rate of used computers, to be positively related to compliance with screen locking procedures, and therefore we hypothesize;

H5A: The ratio of occupied workstations of total workstations per hallway is positively related to compliance with procedures and regulations on the subject of manually locking your screen.

Finally we want to examine how the number of hours worked per day is related to subjects' behaviour regarding compliance with screen locking procedures. The variable number of hours worked per day is a measurement of hours a subject worked on their pc (i.e. the time workstations were locked is reduced of the total number of hours the computer is logged on). Since a higher number of hours worked could be the result of less distracted workers, less meetings etc., we suggest that the number of hours worked is positively related to compliance with screen locking procedures.

H5B: The number of hours worked per day is positively related to compliance with procedures and regulations on the manually locking your screen.

Chapter 3: Research Methods

3.1 Phishing Mail

To test how simulating prior experience with- and providing information about phishing mails affect subsequent behaviour, we conducted a phishing mail field experiment. In this experiment we tested, whether; (1) simulating prior experience with phishing mails, (2) receiving information over phishing mails (infographics), or (3) the combination of both interventions, affect the number of participants falling for phishing mail fraud.

Conducting a phishing mail experiment is somewhat controversial. Because informing the employees upfront about the research would confound the results, we had to make use of deception. Both the use of deception and a complete waiver of informed consent, comprise the controversial elements of conducting a phishing mail field experiment, but where carefully considered and weighed against the risks of information security.

We constructed a legally required Privacy Impact Analysis, in which we stated our possible concerns. Our major concerns were; (1) can an employer 'conduct an experiment on his employees' without informing them upfront (complete waiver of consent), and most important (2) privacy related issues. Therefore we took several precautions, such as; (1) analysing anonymous and aggregated data, (2) stating, prior to the research, the general norm of Information Security System Policy compliance on intranet, (3) informing the Employees Council of the Ministry, (4) debriefing all employees after the research with an elaborate mail, and (5) providing a medium for the employees, to ask questions and/or give comments to the researchers.

3.1.1 Participants

The target population for this experiment were employees of the Dutch Ministry of Economic Affairs (12.567). First we started by excluding those participants with errors/flaws in the dataset. We excluded 40 participants due to their age (age < 16 & age > 70), 17 due to missing organizational unit information and 408 due to missing mail addresses. Furthermore we excluded the departments which are covered by a different IT assistance. Finally some participants were excluded due to their rank in the organization (Minister, State Secretary and Secretary General etc.). After excluding these participants, our subject pool consisted of 10.927 employees. The majority of participants were males (60,6%), with an average age of 47 years (*Table 3.3.*)

3.1.2 Design

Treatment Information

Treatment : Experience

<i>G1 : Control Group</i>	<i>G2: Information provision</i>
<i>G3: Simulated experience</i>	<i>G4: Combined treatment</i>

Table 3.1. *PM:* experimental design

Participants were divided into four equally sized groups (2723, 2740, 2724, 2742), one control- and three treatment groups in which we tested several treatments; (1) information provision, (2) simulating prior experience with phishing mails, and (3) a combination of information provision and simulating prior experience (Table 3.1.).

All the four groups received a 'phishing' mail at T=4. The first treatment group was given three information mails (T=1, T=2 and T=3) with information about; (1) what is phishing, and how does it work, (2) how receivers can recognize phishing mails, and (3) what you should do if you receive a phishing mail. The second treatment group was sent a simulated phishing mail, both at time T=0 and T=4. Furthermore they received a short debriefing explaining that the sent e-mail was fake. No information was given, that emails were part of an experiment. The third treatment group, received both the phishing mail at t=0 and the information mails at T=1, T=2 and T=3. One day after the phishing mail at T=4, all the four groups received a general debriefing.

Table 3.2. PM: Phishing mail experimental procedure.

Group	T = 0 05-11	T = 1 19-11	T = 2 26-11	T = 3 03-12	T = 4 15-12
G1: Control group	-	-	-	-	Phishing mail + debriefing
G2 : Information provision	Phishing mail + short debriefing	Infographic 1	Infographic 2	Infographic 3	Phishing mail + debriefing
G3: Simulating experience	Phishing mail + short debriefing	-	-	-	Phishing mail + debriefing
G4: Combined treatment	Phishing mail + short debriefing	Infographic 1	Infographic 2	Infographic 2	Phishing mail + debriefing

3.1.3 Group formation

We randomized the participants on cluster level of the lowest known organizational unit, 184 unique clusters, with an average of 61.45 participants per cluster. Because we wanted to minimize possible contamination of results by intervention spill over effects, we have not opted perfect randomization. For example, with perfect randomization, it would have been possible that two participants, who work together, are divided into different treatment groups. This may lead to participants being affected by more than one treatment.

Table 3.3. PM: Summary statistics per group

Group	N	Gender		Age	Employee contract			Organisation			
		M	F	Average	Internal	External	AT	RVO	NVWA	KD	DICTU
1	2723	1648	1075	47.4	2184	539		891	920	526	368
2	2740	1673	1067	47.4	2174	566	262	1233	537	373	335
3	2724	1634	1090	47.1	2200	524		1019	738	690	277
4	2742	1666	1076	47.3	2207	535		891	740	769	342

Furthermore randomization based on the five largest organizational divisions of Ministry of Economic Affairs was also excluded, because we expected that organization culture, workplace environment etc. would be of too high influence on human behaviour, possibly leading to contamination of the causal interference of our treatments.

Therefore, with cluster randomization we tried to reduce both; treatment spill over- and division specific effects, while controlling for: (1) age, (2) gender, (3) employee contract (internal/external), and (4) the most equal possible division of the five largest divisions (RVO, NVWA, KD, DICTU, AT). We ran kurskall-Wallis tests to check if these control variables were equal divided between groups. Given a significance level of 2.5% ($\alpha = 2,5$) test results showed no statistically significant differences in groups based on age ($\chi^2=2,479$; $P=0,479$), age-groups ($\chi^2=2,593$; $P=0,459$), gender ($\chi^2= 0,508$; $P=0,917$) or employee contract ($\chi^2= 0,932$; $P=0,818$). However, the difference of the division of the five largest departments is statistically significant different ($\chi^2= 21,256$; $P=0,000$) (*Appendix 3.1*).

3.1.4 Procedure

Phase 1: Pre-intervention period (Group 1-4)

G1	G2	G3	G4
----	----	----	----

In order to assure a certain base line, equal for the four groups, a service notice was posted on the intranet of all the 5 organizational division prior to the experiment, visible to all participants. This message, state the dangers of giving away personal details. Furthermore, the message stated that the Ministry or a division of the Ministry will never ask employees for their password, username etc. (*Appendix 3.2*).

Furthermore, in order to inform/help participants as much as possible during the experiment we made some arrangements with parties, which could be contacted by participants (i.e. IT helpdesk, IS coordinators etc.). We wanted to assure that none of these parties would inform the participants that they were part of an experiment, because this could confound our results. Therefore, we provided them with standardized protocols for mail and phone. This allowed these parties to answer the possible questions of participants, without disturbance of the experiment.

Moreover, at the IT helpdesk a dedicated group of employees was formed, who were in first line of contact with the participants. Participants were redirected to this dedicated group through a choice option at the service line or by automatically forwarding mails to them. Arrangements were made such that when participants phoned or mailed them, they were told standardized answers, which were carefully constructed and suited for each specific question participants could ask. This way, we could; (1) inform/help participants as much as possible, without informing them of the experiment, (2) control the outgoing messages, and (3) monitor the number and type of responses by participants (*Appendix 3.3*).

Phase 2: First phishing mail: simulating experience (Group 3 & 4)

G1

G2

G3

G4

In order to familiarize participants with phishing mails, a simulation phishing mail was designed and sent to participants in group 3 (simulated experience treatment) and group 4 (combined treatment). This way they can gain familiarization and experience in the recognition of phishing mail attacks. On November the fifth, participants received an 'imitation' phishing mail, with topic: "*Economic Affairs – Mobile Password Recovery System*". This mail was sent by operational management, and participants were asked to link their account to their mobile phone number. This Mobile Password Recovery System would enable employees to easily recover its password if it was lost, or to change it.

In order to resemble modern phishing mails, the mail contained several characteristics to enable the receiver to assess the mail as being fake/fraudulent, presenting more or less the same level of difficulty as phishing mails that are actually sent these days. These characteristics were; (1) a misspell in the sender e-mail, (2) inappropriate use of capital letters in the subject line, (3) a change in the logo and logo colour, (4) an unusual form of salutation (for the Ministry), (5) addressing the receiver in the formal V-form instead of the informal T-form, (6) a hyperlink in the mail, referring to a vague website, with an extension that would normally not be used within the Ministry (.net) and (7) two different but resembling fonts, in the main text and disclaimer (*Appendix 3.4*).

Furthermore, we chose an e-mail subject and sender, which we believed to be equally relevant to most participants. The link in the mail, redirected the participant to a 'fake' website (www.mobilepasswordrecoveryssystem.net). This site had a very basic design and contained a few elements of the Governmental visual design style, with some modifications. The only information the participants was given on this site, was; "Koppel in 2 simpele stappen uw gebruikersnaam aan uw mobiele nummer" (Link in two simple steps your username and mobile phone number). In order to link username and phone number, participants were asked to fill in three personal details; (1) username, (2) password, and (3) phone number. After filling in the details, participants were redirected to a second screen, thanking them for the registration and stating that the registration would be completed within five workdays. To complete the registration, it was not necessary to fill in all the three personal details. For example, even if a participant only filled in username (not password and phone number) and clicked on 'send', he or she was directed towards the second screen and was thanked for his registration (*Appendix 3.5*).

Participants who recognized the mail as being fraudulent and send it to the IT helpdesk (of the ministry of Economic Affairs), received an answer stating that the mail was indeed a phishing mail, that the threat had receded, and that no further actions on behalf of the user were needed (*Appendix 3.3*). If participants mailed the IT helpdesk, without adding the mail, they were still asked to send the phishing mail. This was to establish with certainty that the notification indeed concerned our 'imitation' phishing mail and not a 'real-non-experiment-related' phishing mail. Employees who phoned the IT helpdesk to report the 'imitation' phishing mail, were first asked the subject and sender of the mail. Furthermore, if it indeed concerned our mail, they were asked to send the mail as an attachment in an email to the IT helpdesk. Employees who did not see the mail

as suspicious but asked substantive questions regarding the 'mobile password recovery system' were given the answer that they would receive an answer within three workdays (which is standard protocol for all IT related questions) (see *Appendix 3.3* for protocols: standard answers incoming mails and phone calls).

By unique links in the emails, data was collected, on whether the participant; had clicked on the link, and had filled in personal details. Importantly, the content of what participants had filled in was not registered, thus personal details were not recorded. Only whether participants had entered something in one or more (and which) of the fields for personal details, and at what time, was recorded.

At the end of the day the participants received a short debriefing, regarding above mentioned mail. In this debriefing the participants were told that the mail was an 'imitation' phishing mail designed to increase awareness regarding the topic phishing fraud. No further information was given that the mail was part of an experiment or that there would be follow-up actions (*Appendix 3.6*).

Phase 3: Information Provision – Infographics (Group 2 &4)

G1	G2	G3	G4
----	----	----	----

In order to improve knowledge on the topic of phishing mails, participants in group 2 (information provision treatment) and group 4 (combined treatment) received emails with information on ways to avoid falling for phishing attacks. This information provision occurred on a weekly base. In three consecutive weeks, participants received three infographics by mail, regarding information about; (1) what is phishing and how does it work, (2) how receivers could recognize phishing mails, and (3) what actions a receiver should undertake when he/she received a phishing mail (*Appendix 3.7*).

The first information mail starts with a short introduction of the director of operational management. The introduction states that the received mail is part of an information provision campaign, consisting of three information emails. Furthermore the subjects are given information about how phishing fraud works and the newer generation of phishing fraud, spear phishing attacks.

The second information mail starts with a short recap of the first information mail. Furthermore it provides the reader with six points of recognition by which he/she could determine whether emails are fraudulent or not, such as; (1) the mail address of the sender, (2) the salutation, (3) style of writing (grammatical or spelling errors), (4) the hyperlink in the mail, (5) look the sender up on the internet, (6) check the mail address in the signature. Also it lists the types of information that the ministry never will ask their employees. Finally, it states the three largest consequences (for organizations) of phishing fraud.

The third information mail starts again with a short recap of the first two information mails. Furthermore it provides information about, how you should act in the case that (you think that) you have received a phishing mail and how and where you could report a phishing mail. It concludes with some useful links to other (phishing awareness) campaigns of the Dutch Ministry of Economic Affairs (www.veiliginetnetten.nl and iBewustzijn) where more information could be found, including some examples of phishing mails.

Moreover the three infographics had some synergetic power, as each of the three infographics starts with a short recap of the previous mail(s). This ensures the participants that each individual mail is understandable in itself, without necessity of reading them all. Furthermore, the infographics; (1) were readable on the mobile phone, laptop and tablet, (2) did not need to be downloaded first, and (3) were in line with the visual identity style of the Ministry. The story based graphics and annotations, were highly related to the core business activities of the employees and all images/pictures were copyright free, bought or self-made.

Phase 4: Second Phishing mail (Group 1-4)

G1	G2	G3	G4
----	----	----	----

Forty days after participants in group three and four had received a phishing mail, all participants of the four groups received a (2nd) phishing mail. This mail had topic; exceeding the maximum e-mail storage limit, and was sent by the IT department of the Ministry. The participants were told that they had reached their maximum storage limit of Outlook. In order to make sure that the account could still be used for incoming and outgoing e-mail, the limit should be raised. The mail contained a link to www.verhoogjeopslaglimiet.net where employees could raise their mail storage limit (*Appendix 3.8*).

This mail resembled the first mail in; (1) looks, (2) length, and (3) recognizable characteristics of phishing mails. As e-mail is an essential commodity at the Ministry, this required an immediate action of the participants. If they fail to recognize the mail as being 'fraud' and clicked on the link in the mail, they were directed to the website. At this basic site, with some visuals of Outlook Exchange, participants were told that by filling in e-mail, username and password, limits could be raised up to 8 GB. If the participant indeed filled in the details, a pop-up screen was shown, stating that the registration was being processed and that it would be completed within five workdays (*Appendix 3.9*).

Both mail subjects- and senders were chosen to ensure that they represented the types of topics that would be expected in a typical inbox of an employee, as well as the types of institutions that are commonly targeted in phishing mails. Furthermore, the same procedure regarding incoming phone calls and emails was followed as by the first "imitation" phishing mail.

Data was collected on whether the participant; had clicked on the link, and had filled in personal details. Furthermore, which personal details were filled in, accompanied with a timestamp of completion of the registration. What the participants had filled in was not registered, rather only if participants had filled in one or more (and which) fields. No information was given to the participant about the received mail, the related website, and their being fake as a part of an experiment.

Phase 5: Post-intervention period – Debriefing (Group 1-4)

G1 G2 G3 G4

One day after receiving the (second) phishing mail, all participants received a general debriefing. In this elaborate debriefing the participants were told that the phishing mail(s) and information mails were part of an experiment. They were given information about; (1) the cause and purpose of the research, (2) the design of the research, (3) which precautions had been taken in order to respect the privacy of employees- and to protect (personal) details, and (4) where participants could submit other questions- and/or remarks.

Furthermore, they were informed that the experiment was part of the campaign iBewustzijn (Information awareness). With this campaign the Ministry wants to encourage and support its employees as much as possible in developing knowledge and awareness regarding information security. Also it reassured the employees that the phishing mail was fake, such that no consequences were attached if participants indeed had filled in personal details (*Appendix 3.10*).

3.2 Screen locking

Our second experiment regards the topic of screen locking behaviour. As in most companies, there are strict policies at the Ministry regarding for dealing with sensitive information. One of these policies requires that you always should lock your screen, when you leave your workstation. According to the research report "Rapport onderzoek beveiligingskennis van EZ-medewerkers" 84,35 % of the employees knows that you should always lock your screen if you leave your workstation. However a small walk through the building makes it clear that, knowing what should be done and peoples' actual behaviour, are two only slightly overlapping concepts. Furthermore field research revealed that many employees are unaware of how they can quickly lock their screen using the key combinations Windows logo and I key

Currently, as a precautionary measurement to secure sensitive information, each computer at the ministry locks itself automatically after 15 minutes of non-usage. However, ideally employees would lock their computers manually when they leave their computer. Therefore, in this experiment, we test whether providing information and/or emphasizing and reminding the desired behaviour (by placing stickers on keyboards), will lead to more manually locked computers.

3.2.1 Participants

Participants for this experiment were employees of the Ministry of Economic Affairs. However, due to privacy and practical concerns we did not look at behaviour at an individual level, but at pc level. To determine the effectiveness of our experiment and treatments, we analysed data on unique computer serial number related to a fixed location in the main building of the Ministry of Economic Affairs.

3.2.2 Design

Treatment: Information

<i>G1 : Control Group</i>	<i>G2: Information provision (flyer)</i>
<i>G3: Salient reminders (stickers)</i>	<i>G4: Combined treatment</i>

Treatment: Salient reminders

Table 3.4. *SL:* Screen locking experimental design

The (average of used) computers in the main building of the Ministry of Economic Affairs were divided into four 'equally' sized groups (346,322,319,341); one control group and three treatment groups (*Table 3.6*). In these groups we apply three different treatments; (1) information provision by flyers, (2) stickers on the screen and keyboard, and (3) a combination of information provision and stickers. As illustrated by *Table 3.5*, three weeks before the participants received the treatments we started by measuring baseline behaviour. This enabled us to determine the baseline of computer usage for each of the four groups. After the intervention period, treatments were stopped although measuring computer usage was continued in order to determine if changes in behaviour would last. This has also been done two months after the interventions to test if intervention effects are long-lasting.

Table 3.5. *SL:* Screen locking experimental procedure

Group	Pre-Test			Intervention Period		Short-term		Long-term	
	W1	W2	W3	W4	W5	W6	W7	W16	W17
<i>Control Group</i>					-				
<i>Information treatment</i>	Determine the baseline of computer usage for the four groups			Information Flyers		Test whether treatment effect remain		Test whether treatment effect is long-lasting	
<i>Salient reminders</i>				Stickers on Screen and Keyboard					
<i>Combined treatment</i>				Stickers on Screen and Keyboard & Information Flyers					

3.2.3 Group formation

Table 3.6. *SL:* (average occupied) pc's per treatment group

Treatment groups	Number pc's (Average occupied pc's)
Control	523 (346)
Information provision treatment (A-5 flyers)	472 (322,9)
(constant) salient reminders	484 (319,4)
Combined treatment	535 (341,9)
<i>Total</i>	<i>2014 (1330,2)</i>

As mentioned before, we analysed computer usage at computer level and not at individual level. Officially, the building we used consists of flexible workstations, meaning that in practice, different participants could use the same workstation during the experiment. However, we used cluster randomization on hallways and organizational units, meaning that we expect that participants would only switch between computers at a particular hallway, since each department is assigned to a specific hallway. Therefore we expect the effect of participants who are affected by more than one treatment to be limited.

We started by mapping each computer in the building and linked each computer to a unique id in order to link a specific location to a particular workstation. Secondly, we determined the hallway average workstation usage. In other words we logged for two weeks (10 workdays) how many computers in each hallway were used on average. It turned out that there are large differences between hallways in average workstation usage, especially on Wednesdays and Fridays. We used cluster randomization at hallway level in order to diminish possible intervention spill over. We excluded hallways with limited access due to security reasons, both out of practical reasons as also because we believed that those hallways may have higher than average standards of manually screen locking behaviour. Furthermore we excluded some workstations which are used by high ranked employees in the organization (Minister, State Secretary, and Secretary General etc.)(Appendix 3.11).

In total our sample consisted of 57 hallways, with an average of 38 workstations per hallway, of which on average 26,2 workstations were used. We equally divided the different organizational units and hallways among our four groups, hereby also limiting organizational specific effects. Finally the groups in our sample where; (1) G1: control group, 346,0 (523), (2) G2: information provision treatment, 322,9 (472), (3) G3: (constant) salient reminder treatment, 319,4 (484), and (4) G4: combined treatment, 341,9 (535) (The first number is the average of used workstations and the second number between brackets is the total number of workstations).

3.2.4 Procedure

Phase 1: Pre-testing

G1	G2	G3	G4
----	----	----	----

To measure the number of times a computer is manually locked, a tool was developed that logged computer usage behaviour. The tool registers when computers are manually locked and when they are automatically locked (after 15 minutes of computer non-usage). To account for possible differences in baseline of computer usage, we ran a three week pre-test. To assess actual computer usage behaviour as realistically as possible, participants were given no information that computer usage was monitored.

Phase 2: Intervention period

G1	G2	G3	G4
----	----	----	----

Information Flyers

Participants in the information provision treatment (G2: information provision treatment & G4: combined treatment) received educational flyers on screen locking. For two consecutive weeks, information flyers were placed at the workstations of participants, on Monday and Wednesday mornings before 07:00 am. The information flyers were placed upon the keyboards in order to make sure that every participant actually saw the flyers and that they were not removed by cleaning.

The information flyers contained information regarding;

- The keyboard shortcut, to quickly lock your screen (windows logo + L)
- A social norm (84,35 percent of the EZ-employees knows that you should always lock your screen if you are leaving your workplace)
- The dangers / necessity of locking your screen
- A redirection toward extra information and the "Ibewustzijn" campaign of the Ministry.

Also the slogan (*Figure 3.1*) that we developed for our experiment was presented on the flyer. The A5 size flyer was designed to be in line with the standards of visual representation of the Ministry of Economic Affairs and all flyers were removed after two weeks (*see Appendix 3.12: A5-Flyer screen locking (Information intervention)*) Participants were given no information that computer usage was monitored.



Figure 3.1: SL: Slogan information campaign

Emphasizing desired behaviour – Salient reminders

G1	G2	G3	G4
----	----	----	----

In order to make the keyboard shortcut to quickly lock your screen (windows-logo + L) more visually salient, we placed green stickers on the windows and "L" keys of the keyboards of workstations in group 2 (constant salient reminder treatment) and group 4 (combined treatment). In order to make sure that participants actually understood that these two green stickers where to emphasize how to quickly lock your screen, a third green sticker was placed in the right lower corner of the screen. This third sticker contained the slogan for our experiment (Windows Logo + L = Veilig & Snel) with a lock symbol (*see Appendix 3.13: Stickers screen locking (sticker intervention)*).



Figure 3.2. SL: Sticker treatment condition - (constant) salient reminders

Stickers were placed upon the keyboards the Friday night prior to the experiment. Because stickers would be removed after the two weeks intervention period, temporary adhesive stickers were chosen. During the intervention period of the experiment, two times, eventual missing or removed stickers were replaced, to make sure that intervention effect was not diminished. We chose to limit the replacement of stickers to two times, because we also did not want to frustrate participants. Some participants told us that they found the stickers unpleasant to work with. Both times of replenishment, approximately 10-15% of the stickers on the keyboards were removed. Just in a couple of cases the sticker on the screen was also removed. Due to low percentage of missing stickers, two times sticker replenishment, and since stickers were placed on all of the workstations in a particular hallway, we believe the possible diminished effect of missing stickers is negligible. Participants were given no information that computer usage was monitored.

Phase 3: Short-term Post-test

G1	G2	G3	G4
----	----	----	----

After the two week intervention period, computer usage continued to be monitored in order to determine if intervention effect(s) would remain. We removed all stickers and flyers and maintained monitoring computer usage behaviour for another two weeks.

Phase 4 – Determine long-lasting effect – Long-term post-test

G1	G2	G3	G4
----	----	----	----

Eight weeks after treatments were stopped, we restarted monitoring computer usage. In two consecutive weeks we tested whether the treatment effect would last. Again, participants were not told (thus unaware) that computer usage was monitored.

3.3 Recap

In this section we have described the research methods of our two experiments. In short, in the **phishing mail** experiment we want to test whether giving information over- or simulating experience with phishing mails, could reduce susceptibility towards phishing fraud. As precautions we (1) constructed a legally required Privacy Impact Assessment, (2) posted a service notice on intranet (never give up your personal details, in particular your password), and (3) made arrangements in coordination with IT supportive parties. Participants were employees of the Ministry of Economic Affairs. Four treatment groups were formed based on randomization on lowest know cluster level; (1) control group, (2) information provision group (infographics), (3) simulated experience group (prior phishing mail), and (4) combined treatment of information and simulated experience. After the final phishing mail was send, all participants received an elaborate mail with the procedure, scope, cause and aim of the experiment.

Second, in the **screen locking** experiment we want to test whether giving information about screen locking or emphasizing desired behaviour is effective in improving screen locking behaviour (e.g. increasing the number of manually locked screens). A tool was developed which registered computer usage and participants' locking behaviour. Participants were employees stationed at the main building of the Ministry of Economic Affairs. Four treatment groups were formed based on randomization on hallway level; (1) control group, (2) information provision treatment (A5-flyers); (3) constant salient reminders (stickers); and (4) combined treatment of flyers and stickers. First we started by determining baseline levels of participants in a two week pre-test. Secondly, in the following two weeks participants received above mentioned treatments. Moreover, short-term lasting effects were determined the two subsequent weeks after treatments have stopped. Finally, long-lasting treatment effects were determined eight weeks after treatments have stopped.

In the next chapter we will present the results of our findings in which we will state the units of measurement (what-and how is being measured), and all relevant findings. Also other (unanticipated) findings will be presented.

Chapter 4: Results

In this section we present the results of our two field experiments, of which we start with the phishing mail experiment. Since the phishing mail send at $t=1$ (send to participants in treatment 2 and 3; with topic: EZ-Mobile Password Recovery System, only was send to simulate previous experience with phishing emails, only data is presented of the phishing mail which was send to all participants, at $T=4$ (with topic: exceeding the maximum e-mail storage limit). First we discuss an event that contaminated our experiment, and due to which we had to exclude participants of one organizational unit. Moreover our units of measurements are discussed and an overview of the demographic factors of participants is presented as well as some first summary results. Furthermore we will discuss differences in results due to the effects of treatments and organizational units. Afterwards, we will analyse the results of our regression analysis and end the result section of our phishing mail experiment with some final results (incoming complaints/questions and timestamps of the events).

4.1 Phishing mail

4.1.1 Contamination of the experiment and implications

Unfortunately after the first phishing mail was send an event occurred that had large impact on the rest of the experiment. In one of the five largest organizational divisions of the ministry, the NVWA, a notification was posted online that the phishing mail was a fake phishing mail. Therefore also participants in the control group and the information provision treatment received this notification and intervention spill over effects may have occurred. As result, data analysis was done both for the situation where that specific division (NVWA) was included and excluded. Differences in results were found in the analysis (which we discuss in section 4.1.7 and *Appendix 4.1.*, causing the decision to exclude that organizational unit in the analysis for this thesis. This exclusion had as implication that; (1) group size, (2) gender proportion, (3) average age, and (4) employee contract proportion, became less equally divided among the four groups. Furthermore this reduced our sample size by 2935, from 10929 to 7994.

4.1.2 Measuring falling for phishing fraud

We consider two measurements for someone to have fallen for a phishing attack. The *first*, measure is based on clicking on the link in the phishing mail and visiting the site, regardless of whether participants filled in personal details at the 'fake' website. In our research, 62,04 percent of the employees who clicked on the link in a phishing mail provided (personal) information on the 'fake' website. Furthermore, clicking on a link embedded in a phishing mail can be very dangerous, because this link can be used by phishers to infect computers with malware. The link may take victims to a website that infects their computer with malware or it might even download the virus directly without going to a web page. In the remainder of this thesis, this measurement will be addressed as 'visiting the site' or 'clicked on the link'.

The *second* measurement is whether participants actually have filled in personal information on the 'fake' website. This is the most commonly used phishing attack strategy in order to gain personal information of victims. In our experiment, participants could fill in three personal details at the fake websites; Mail 1; (1) username, (2) password, (3) mobile phone number, and Mail 2; (1) username, (2) password, and (3) e-mail address.

As mentioned in *chapter 3*, it was also possible for participants to fill in incomplete registration. Meaning, if a participant had filled in less than three fields, she could still proceed to the next screen, without a warning notification of incompleteness. We deliberately allowed this to happen, since we were interested to see whether there are differences between personal details someone is more likely to fill in. For example, we thought that participants would be more likely to fill in user name or email address, compared to password. In this experiment however, in 99.2% of the cases a participant filled in personal details, she also filled in the password. Therefore we will take the variable password-filled-in as our second measurement for someone who has fallen for a phishing attack.

To summarize, data was collected; (1) if a participant had clicked on the link in the mail/ visited the fake website, (2) if a participant had filled in personal details at the fake website, (3) how many- and which fields were filled in by participants, and (4) at what moment these actions had taken place (timestamp). Furthermore, no data was collected on how many participants had read or opened the information mails. The two above mentioned measurements of being deceived by phishing fraud will be considered as our dependent variables. Furthermore the dataset contains for each participant; Age (in years), gender (M/V), Employee contract (Int./Ext.), Organizational Unit(RVO, KD, DICTU, AT), Group (Control Group, Treatment 1, Treatment 2, Treatment 3¹), visited the site (YES/NO), number of fields filled in (1,2,3), filled in Username (YES/NO), Filled in Password (YES/NO), Filled in E-mail (YES/NO) and a timestamp (Date & Time).

4.1.3 Demographics:

Table 4.1. *PM:* Demographic factors of participants per treatment group

Group	N	Gender		Age	Employee contract		Organisation			
		M	F	Average	Internal	External	AT	DICTU	KD	RVO
1: Control group	1803	60,7%	39,3%	47,4	70,3%	29,3%	-	21,4%	29,2%	49,2%
2: Information provision	2203	56,8%	43,2%	47,5	74,6%	11,9%	11,9%	15,2%	16,9%	55,9%
3: Simulated experience	1986	58,9%	41,1%	46,1	74,4%	25,6%	-	13,9%	34,7%	51,3%
4: Combined treatment	2002	60,2%	39,8	46,7	73,5%	26,5%	-	17,8%	38,4%	44,51%
Average		59,7%	40,9%	46,5	73,3%	26,7%		16,7%	29,5%	50,5%

¹ Treatment 1= information (provision treatment), Treatment 2= (simulated) experience (treatment) and Treatment 3= combined (treatment).

Table 4.1 summarizes descriptive statistics per group. The demographic data shows that the percentages of males (59,7%), the average age (46,5) and employee contract (73,3%) are rather equally distributed among the four treatment groups. We see however, in Figure 4.1, large differences in the distribution of age for males and females, particular for the group older than 45 years. We observe a decline of women in the groups 46-55 and 55+. However, compared to men, we see an increase in number of males falling in the age categories 46-55 and 55+. The average age of males (48,0) is close to four years older than females (44.3). The distribution of age for males is; 16-25 (1,9%), 26-35 (12,4%), 36-45 (27,5%), 46-55 (32,2%), 55+(26,0%) and for females; 16-25(11,9%), 26-35 (16,1%), 36-45(32,1%), 46-55 (16,1%) and 55+ (11,9%).

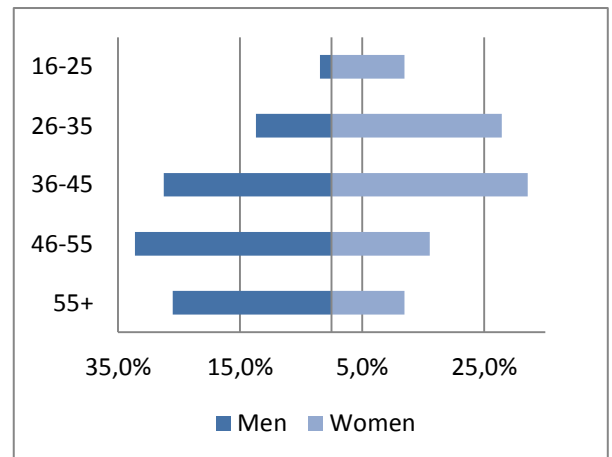


Figure 4.1. PM: Participants' age distribution by gender.

Most of the participants fall under the organizational unit RVO (50,5%) followed by, KD (29,5%), DICTU (16,7%) and, the smallest organizational unit, AT (3,3%). These are however not equally divided per treatment group, due to randomization on cluster level (Appendix 4.2).

4.1.4 First results - Treatments

Table 4.2. PM: Number of participants falling for phishing fraud per condition (in exact numbers and percentages).

Group	N	Visit the site	Username	E-mail	Password
Control group	1803	584 – 32,4%	402 – 22,1% (68,8%) *	401 – 22,2% (68,7%)	399 – 22,1% (68,3%)
Information provision	2203	530 – 24,1%	321 – 14,6% (60,6%)	321 – 14,6% (60,6%)	320 – 14,5% (60,4%)
Simulated experience	1986	384 – 19,3%	214 – 10,8% (55,7%)	214 – 10,8% (55,7%)	212 – 10,7% (55,2%)
Combined treatment	2002	449 – 22,4%	246 – 12,3% (54,8%)	246 – 12,3% (54,8%)	242 – 12,1% (53,9%)
Total	7976	1947 – 24,4%	1183 – 14,8% (60,8%)	1182 – 14,8% (60,7%)	1173 – 14,7% (60,2%)

*(percentage of participants filling in personal details of those who visited the link)

As shown in Table 4.2, and Figure 4.2 and 4.3, on average, 24,4% of the participants have visited the site and 14,7% have filled in their password on the website. Participants in the control group most frequently failed to recognize that the received mail was a phishing mail. Almost one third of the participants (control group) visited the link and 22,1% entered their password on the registration form. Comparing the control group with the treatment groups, we observed a decline in participants who falls for phishing attacks for all three treatments. Looking at both measurements of falling for phishing fraud, the fewest participants falling for phishing attacks are in the simulated previous experience treatment. Furthermore we observed small differences in results between the simulated previous experience treatment and the combined treatment.

4.1.5 Treatment Differences

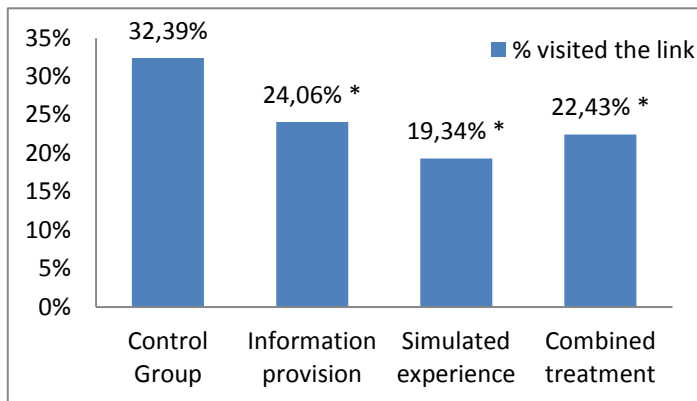


Figure 4.2. PM: Percentage of participants who visited the site per treatment (* significantly different compared to the control group).

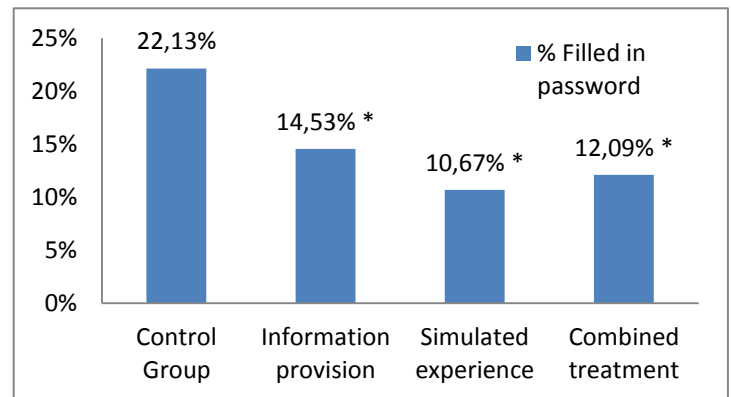


Figure 4.3. PM: Percentage of participants who filled in their password per treatment (* significantly different compared to the control group).

In order to test the significance of differences in results, we performed Fischer exact tests and Chi-Squared tests. We ran the tests for both measurements of being deceived by a phishing mail (visit the site/clicked on the link & filled in password) (Table 4.3 & 4.4).

Table 4.3. PM: Overview χ^2 test results - Participants Visited the link in the mail per treatment

	Information	Experience	Combined
Control	$\chi^2=34,291$; P= 0,000***	$\chi^2=84,680$; P= 0,000***	$\chi^2=47,609$; P= 0,000***
Information		$\chi^2=13,656$; P= 0,000***	$\chi^2=1,561$; P= 0,211
Experience			$\chi^2=5,769$; P= 0,016**

* P<0,10 **P<0,05 *** P<0,01

Table 4.4. PM: Overview χ^2 test results - Participants filled in their password per treatment

	Information	Experience	Combined
Control	$\chi^2=38,931$; P=0,000***	$\chi^2=91,685$; P=0,000***	$\chi^2=68,289$; P=0,000***
Information		$\chi^2=13,970$; P=0,000***	$\chi^2=5,383$; P=0,021**
Experience			$\chi^2= 1,974$; P=0,163

* P<0,10 **P<0,05 *** P<0,01

In all three treatment groups, fewer participants fall for phishing fraud compared to the control group. This holds for both the number of participants visiting the link (T1: $\chi^2=34,29$; P<0,001, T2: $\chi^2=84,68$; P<0,001, T3: $\chi^2=46,61$; P<0,001) as filled in passwords (T1: $\chi^2=38,93$; P<0,001, T2: $\chi^2=91,69$; P<0,001, T3: $\chi^2=68,29$; P<0,001). Therefore, in this sample, providing information about phishing, simulating experience with phishing mails and combining both treatments, reduced the number of participants who fall for phishing attacks (p<0,001)(Table 4.3 and 4.4).

Furthermore as shown in *Table 4.3* and *4.4* some treatments reported to be more or less effective in reducing the number of participants who filled in passwords or visited the 'fake' website. For both visiting the site as filling in password, the number of participants falling for phishing fraud, is significantly higher in the information provision treatment compared to the simulated experience treatment (M1²: $\chi^2=13,66$; $P<0,001$, M2³: $\chi^2=13,97$; $P<0,001$). By comparing the information provision treatment with the combined treatment, we observed no significant differences in the number of participants who visited the site (M1: $\chi^2=1,56$; $P=0,211$). However, the number of participants who filled in their passwords is significantly lower in the combined treatment compared to the information provision treatment (M2: $\chi^2=5,38$; $P=0,021$). Additionally, the number of participants who visited the site is significantly higher in the combined treatment, compared to the simulated experience treatment (M1: $\chi^2=5,769$; $P=0,016$). Although, differences between both treatments are insignificant regarding the number of participants who filled in passwords (M2: $\chi^2=1,974$; $P=0,163$).

Finally we investigated whether there is any treatment effect on the number of participants who continued with filling in the password after they have visited the site (i.e. whether treatments would affect the (dis)continuation of filling in personal details, after the participants had viewed the website). As shown in *Table 4.5*, all differences in results are significant except for the difference between the information provision treatment and simulated experience treatment ($\chi^2=2,45$; $P=0,118$), and the simulated experience treatment and the combined treatment ($\chi^2=0,14$; $P=0,705$) ($p<0,05$) (*Figure 4.5*).

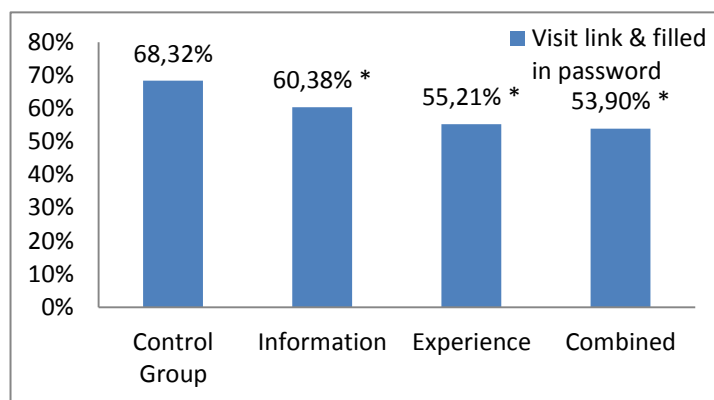


Figure 4.4. PM: Percentage of participants who filled in password of those who clicked on the embedded link (* significantly different compared to the control group)

Table 4.5. PM: Overview χ^2 test results- Participants who filled in their password of those who clicked on the link embedded in the phishing mail.

	Information	Experience	Combined
Control	$\chi^2=7,66$; $P=0,006^{***}$	$\chi^2=17,11$; $P=0,000^{***}$	$\chi^2=22,43$; $P=0,000^{***}$
Information		$\chi^2= 2,45$; $P=0,118$	$\chi^2= 4,17$; $P=0,041^{**}$
Experience			$\chi^2= 0,14$; $P=0,705$

* $P<0,10$, ** $P<0,05$, *** $P<0,01$

² Measurement 1 (M1)= visited the site or clicked on the link.

³ Measurement 2 (M2)= filled in password.

Table 4.6. PM: Participants visiting the link, per treatment (in exact numbers and percentages). Number of observations, gender, age, employee contract and organizational division distribution.

Group	N	Gender		Age	Employee contract		Organization			Overall	
		Male	Female	Average Age	Internal	External	AT	RVO	KD		DICTU
1 : Control group	<u>1803</u>	<u>1094</u> ⁴	<u>709</u>	<u>47,4</u>	<u>1267</u>	<u>536</u>		<u>891</u>	<u>526</u>	<u>368</u>	<u>1785</u>
		369 ⁵	215	48,1	434	150		266	194	124	584
		33,73% ⁶	30,32%		34,25%	27,99%		29,90%	36,90%	32,10%	32,72%
2: Information provision	<u>2203</u>	<u>1252</u>	<u>951</u>	<u>47,4</u>	<u>1643</u>	<u>560</u>	<u>262</u>	<u>1233</u>	<u>373</u>	<u>335</u>	<u>2203</u>
		336	194	47,5	418	112	89	258	87	96	530
		26,84%	20,40%		25,44%	20,00%	34,00%	20,90%	23,30%	28,70%	24,33%
3: Simulated experience	<u>1986</u>	<u>1170</u>	<u>816</u>	<u>47,1</u>	<u>1478</u>	<u>508</u>		<u>1019</u>	<u>690</u>	<u>277</u>	<u>1986</u>
		248	136	48,5	312	72		189	153	42	384
		21,20%	16,67%		21,11%	14,17%		18,60%	22,20%	15,20%	19,33%
4 : Combined treatment	<u>2002</u>	<u>1206</u>	<u>796</u>	<u>47,3</u>	<u>1472</u>	<u>530</u>		<u>891</u>	<u>769</u>	<u>342</u>	<u>2002</u>
		277	172	49,0	332	117		194	173	82	449
		22,97%	21,61%		22,55%	22,08%		21,80%	22,50%	24,00%	22,43%
Overall	<u>7994</u>	<u>4772</u>	<u>3272</u>	<u>46,5</u>	<u>5860</u>	<u>2134</u>	<u>262</u>	<u>4034</u>	<u>2358</u>	<u>1340</u>	
		1230	717	48,2	1496	451	89	907	607	344	
		25,78%	21,91%		25,53%	21,13%	34,00%	22,48%	25,74%	25,67%	

⁴ Total number of participants

⁵ Number of participants who visited the site / clicked on the link

⁶ Percentage of participants who visited the site/ clicked on the link of total number of participants

Table 4.7. PM: Participants filling in their password, per treatment (in exact numbers and percentages). Number of observations, gender, age, employee contract and organizational division distribution.

Group	N	Gender		Age	Employee contract		Organization			Overall	
		Male	Female	Average Age	Internal	External	AT	RVO	KD		DICTU
1 : Control group	<u>1803</u>	<u>1094</u> ⁷	<u>709</u>	<u>47.4</u>	<u>1267</u>	<u>536</u>		<u>891</u>	<u>526</u>	<u>368</u>	<u>1785</u>
		251 ⁸	148	48.6	295	104		187	134	78	399
		22,94% ⁹	20,87%		23,28%	19,40%		20,99%	25,48%	21,20%	22,35%
2: Information provision	<u>2203</u>	<u>1252</u>	<u>951</u>	<u>45.7</u>	<u>1643</u>	<u>560</u>	<u>262</u>	<u>1233</u>	<u>373</u>	<u>335</u>	<u>2203</u>
		199	121	48,6	259	61	65	160	44	51	320
		15,89%	12,72%		15,76%	11,09%	24,81%	12,98%	11,80%	15,22%	14,53%
3: Simulated experience	<u>1986</u>	<u>1170</u>	<u>816</u>	<u>46.1</u>	<u>1478</u>	<u>508</u>		<u>1019</u>	<u>690</u>	<u>277</u>	<u>1986</u>
		133	79	49.6	171	41		101	93	18	212
		11,37%	9,68%		11,57%	8,07%		9,91%	13,48%	6,50%	10,67%
4 : Combined treatment	<u>2002</u>	<u>1206</u>	<u>796</u>	<u>46.7</u>	<u>1472</u>	<u>530</u>		<u>891</u>	<u>769</u>	<u>342</u>	<u>2002</u>
		139	103	49.8	180	62		107	97	38	242
		11,53%	12,94%		12,28%	11,70%		12,01%	12,61%	11,11%	12,09%
Overall	<u>7994</u>	<u>4772</u>	<u>3272</u>	<u>46.5</u>	<u>5860</u>	<u>2134</u>	<u>262</u>	<u>4034</u>	<u>2358</u>	<u>1340</u>	
		722	451	49,0	905	268	65	555	368	185	
		15,13%	13,78%		15,44%	12,56%	24,81%	13,76%	15,61%	13,81%	

⁷ Total number of participants

⁸ Number of participants who filled in password

⁹ Percentage of participants who filled in password of total number of participants

4.1.6 Regression analysis

To explore factors that predict the probability of being deceived by phishing attacks, we performed logistic regressions. This section explains the steps we took to build the model and discusses the results from the logistic regression. We divided this section into two subsections, one for each of the dependent measurements; (1) filled in password and (2) visited the link.

We ran logistic regressions predicting the vulnerability of being deceived (for both measurements) by phishing attacks. In *Table 4.10* & *4.11* we report variables that are statistically significant at $p \leq 0,05$. To measure the likelihood participants clicked on the link embedded in the phishing mail, we ran a logistic regression with independent variables; gender (male), employee contract (Int_Employee), treatments (Group(1-4)), (d_organisatieonderdeel(A,D,M,R)) and age categories (16-25;26-35;36-45;46-55;56+). We ran both logit and probit regression and found no differences in sign and significance for the independent variables (*Appendix 4.3., 4.5. and 4.6.*).

Measurement 1: Visited the site

Table 4.8. PM: Y= M2_VisitlinkBin (visited the site). Logistic regression analysis with parameters, standard errors, confidence interval, odds ratio's and marginal effects (significant at $p \leq 0,05$).

Variable	β	SE	Percentile 95% CI		Odds Ratio	Margin (dy/dx)
			Lower	Upper		
Male	0,163	0,057	0,050	0,275	1,177	0,029
Int_Employee	0,154	0,070	0,018	0,290	1,166	0,027
Information treatment	-0,419	0,075	-0,566	-0,272	0,658	-0,083
Experience treatment	-0,667	0,077	-0,817	-0,516	0,513	-0,125
Combined treatment	-0,502	0,074	-0,647	-0,356	0,605	-0,098
Organization D	-0,339	0,158	-0,649	-0,029	0,713	-0,068
Organization M	-0,327	0,150	-0,620	-0,033	0,721	-0,066
Organization R	-0,481	0,145	-0,765	-0,198	0,618	-0,094
age_group2 (36-45)	0,489	0,236	0,026	0,952	1,630	0,072
age_group3 (46-55)	0,809	0,236	0,347	1,271	2,246	0,131
age_group4 (55+)	0,763	0,238	0,296	1,231	2,145	0,122

Men significantly clicked more on the link embedded in the mail, compared to women. Being male increases the odds of visiting the link by 17,65% ($Z=2,83$; $P=0,005$), an average of 25,78% compared to 21,91% for females ($\chi^2=17,94$; $P<0,001$) ceteris paribus. Furthermore we examined the effect of being an internal – or external employee. We observed that being an internal employee increases the odds of visiting the site by 16,64% ($Z=2,21$; $P=0,027$), an average of 25,53% compared to 21,13% for external employees ($\chi^2=16,40$; $P<0,001$) ceteris paribus.

Moreover, we analysed the effect of differences in treatments and found the odds of being deceived by a phishing mail is lower for participants of all treatments, compared to the control group ($p < 0,05$). We observed decreased odds of being deceived for; (1) Information provision 34,24% ($Z = -5,59$; $P < 0,001$); (2) simulating previous experience 48,67% ($Z = -8,69$; $P < 0,001$), and (3) the combined treatment 39,46% ($Z = -6,76$; $P < 0,001$). The number of participants clicked on the link is significantly lower for participants in the simulated previous experience treatment, compared to information provision treatment ($\chi^2 = 9,65$; $P = 0,000$), and for participants in the simulated experience treatment compared to the combined treatment ($\chi^2 = 4,41$; $P = 0,036$). The differences between the information provision treatment and the combined treatment ($\chi^2 = 1,13$; $P = 0,288$) is insignificant ($P > 0,05$).

Table 4.9. PM: Overview Wald- χ^2 test results- Participants visited the sited/ clicked on the link

	Information	Experience	Combined
Control	$\chi^2 = 31,21$; $P = 0,000^{***}$	$\chi^2 = 75,44$; $P = 0,000^{***}$	$\chi^2 = 45,64$; $P = 0,000^{***}$
Information		$\chi^2 = 9,65$; $P = 0,002^{***}$	$\chi^2 = 1,13$; $P = 0,288$
Experience			$\chi^2 = 4,41$; $P = 0,036^{**}$

* $P < 0,10$, ** $P < 0,05$, *** $P < 0,01$

Furthermore, we investigated the effect of age on the likelihood participants visited the site. To do so, we spread age over five age categories (16-25; 26-35; 36-45; 46-55; 55+), of which the youngest age category (16-25), is the reference category. Being aged 26-35 increases the odds of visiting the link with 63,03% ($Z = 2,07$; $P = 0,039$), aged 46-55 with 124,59% ($Z = 3,43$; $P = 0,001$) and aged 55+ with 114,54% ($Z = 3,20$; $P = 0,001$). The effect of being aged 26-35 is insignificant ($p > 0,05$) (*Appendix 4.4.*).

Finally we looked at the effects of differences in organizations. We found significant differences between AT and; (1) DICTU, (2) KD (3) RVO. However, we advise cautiousness with interpreting results of the organizational unit AT, as it is a relatively small group compared to the other divisions and participants could not be divided over all treatments, as shown in *Table 4.1, 4.8* and *4.9* (only in the information provision treatment). Although, we still report results for completeness and included the variables to correct for differences between divisions in the regression analysis. Comparing the effect of organizational divisions we observed that the odds of visiting the site decreases for; (1) DICTU with 28,73% ($Z = -2,14$; $P = 0,032$), (2) KD with 27,86% ($Z = -2,18$; $P = 0,029$) and (3) RVO with 38,2% ($Z = -3,33$; $P = 0,001$) *ceteris paribus*.

Measurement 2: Filled in Password

Table 4.10. PM: $Y = M2_Password$ (filled in password). Logistic regression analysis with parameters, standard errors, confidence interval, odds ratio's and marginal effects (significant at $p < 0,05$).

Variable	β	SE	Percentile 95% CI		Odds Ratio	Margin (dy/dx)
			Lower	Upper		
Information treatment	-0,570	0,089	-0,745	-0,395	0,564	-0,081
Experience treatment	-0,848	0,093	-1,031	-0,665	0,428	-0,111
Combined treatment	-0,727	0,090	-0,903	-0,551	0,484	-0,099
Organization D	-0,717	0,182	-1,073	-0,361	0,488	-0,103
Organization M	-0,567	0,169	-0,898	-0,236	0,567	-0,085
Organization R	-0,679	0,162	-0,998	-0,361	0,507	-0,099
age_group 3 (46-55)	0,679	0,288	0,114	1,244	1,971	0,073
age_group4 (55+)	0,794	0,291	0,224	1,365	2,213	0,093

We also ran logistic regression for the second measurement of falling for phishing attacks, filled in password (*Appendix 4.7., 4.9. and 4.10.*). Compared to the first measurement, visited the site/clicked on the link, the effect of gender and employee contract on the likelihood of filling in password is insignificant ($P > 0,05$). An average of 13,78% for females, compared to 15,13% for males ($\chi^2 = 3,50$; $P = 0,061$), and 12,56% for external employees compared to 15,44% for internal employees ($\chi^2 = 10,40$; $P < 0,001$).

Again, we analysed the effect of differences in treatments and found the odds of filling in password is lower for participants of all treatments, compared to the control group ($P < 0,05$). We observed decreased odds of being deceived for; (1) the information provision treatment: 43,45% ($Z = -6,39$; $P < 0,001$); (2) the simulated previous experience treatment: 57,17% ($Z = -9,10$; $P < 0,001$) and (3) the combined treatment: 51,65% ($Z = -8,09$; $P < 0,001$). Contrary to findings presented at the first measurement (visiting the site) regression analysis, only differences between the simulated previous experience treatment and the combined treatment, reported to be insignificant ($\chi^2 = 1,46$; $P = 0,227$). Therefore participants in the information provision treatment are more likely to fill in their password, compared to the simulated previous experience treatment ($\chi^2 = 7,68$; $P = 0,006$) and combined treatment ($\chi^2 = 4,21$; $P = 0,040$).

Table 4.11. PM: Regression analysis- Overview Wald- χ^2 test results- Participants filled in password

	Information	Experience	Combined
Control	$\chi^2 = 40,88$; $P = 0,000^{***}$	$\chi^2 = 82,81$; $P = 0,000^{***}$	$\chi^2 = 65,39$; $P = 0,000^{***}$
Information		$\chi^2 = 7,68$; $P = 0,006^{***}$	$\chi^2 = 4,21$; $P = 0,040^{**}$
Experience			$\chi^2 = 1,46$; $P = 0,227$

* $P < 0,10$, ** $P < 0,05$, *** $P < 0,01$

Furthermore, age category comparisons are investigated. Being aged 46-55 increases the odds of filling in password with 97,15% ($Z=2,37$; $P=0,019$), this is even higher for participants aged 55+ ((121,32%) ($Z=2,73$; $P=0,006$)). With respect to the reference category (age 16-25), differences in the number participants who filled in password are insignificant for age category 1 (aged 26-35($Z=0,06$; $P=0,954$) and age category 2 (aged 36-45($Z=0,88$; $P=0,381$)). Finally we looked at the effects of differences in organizations. We found significant differences between AT and; (1) DICTU, (2) KD, and (3) RVO. Comparing the effect of organizations we observed that the odds of filling in your password decreases with; (1) 51,19% DICTU ($Z=-3,95$; $P<0,001$), (2) 43,29% for KD ($Z=-3,36$; $P=0,001$), and (3) 49,31% for RVO ($Z=-4,18$; $P<0,001$) compared to AT, ceteris paribus. Again we advise cautiousness by interpreting these results.

4.1.7 Comparing results with & without the exclusion of the NVWA

In this section we only present differences treatments effectiveness (comparison). In above shown results, we found significant differences for the number of participants who clicked on the embedded link in the phishing mail. This applies to the experience treatment compared with both the information treatment and combined treatment ($P<0,05$). However, differences are insignificant when the NVWA is included in our regression analysis ($P>0,10$). A more detailed overview of differences in results with and without the NVWA can be found in *Appendix 4.1.*

4.1.8 Other results

We end this section by providing other results of our experiment. As illustrated in *Figure 4.5.* and 4.6 more than 80 percent of the participants who were deceived by the phishing attack, were so within three hours. We set $t=0$ at 09:00 hour, just a couple of minutes before the phishing mail was send. Also, we registered call and mail correspondence of participants with the IT helpdesk. To ensure participants were given no information about the experiment, a dedicated group of employees was formed, who dealt with the correspondence with participants. This way we approached the situation of a phishing mail as realistic as possible. In total, the IT helpdesk was phoned 787 and mailed 1407 times. However, since participants who phoned the IT helpdesk also were asked to send the question by mail, we assume high overlap of incoming calls and mails. Due to privacy concerns these calls and mails could not be more specified or related to treatments and/or organizational units. As implication, these variables could therefore not be included as control variables in our regression analysis.

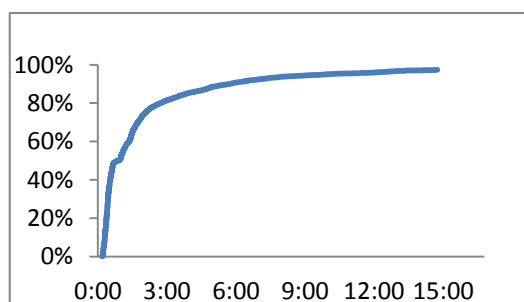


Figure 4.5. PM: Visit the site (T=0) , responses over time (send 09:00).

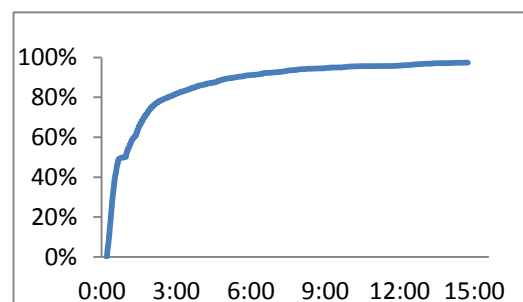


Figure 4.6. PM: Filled in password responses over time. (send 09:00).

4.2. Screen locking

In the remainder of this chapter we present the results of our screen locking experiment. The outline for this section is as follows. We start by stating how and what we have measured. Moreover we will provide the results of treatment effects on screen locking behaviour per pure hour worked. Furthermore results of the ratio manual locks to total locks will be discussed. Finally we conclude with the results of our regression analysis of the main -and extended model.

4.2.1 Measuring screen locking behaviour

We have determined two measurements for the number of manual locks, namely per day per pc and per hour worked per pc. We have subtracted the time a computer is locked from the total time a computer is logged on, in order to determine the pure working time per computer. However as shown in *Appendix 4.11*. total pure working time and average pure working time per day per pc are quite different between groups. Therefore we propose to analyse results based on locks per hour worked instead of per day.

The tool we let develop logged for each computer per day whether it has been; (1) turned on/off, (2) logged on/off, (3) locked manually/automatically, and (4) unlocked. These variables allow us to determine the number of manual locks per hour worked and the ratio manual locks to total locks. Furthermore our dataset contains information about; (1) which hallway the computer was located, (2) how many computers per hallway per day were used, (3) organizational unit per hallway, (4) number of hours the computer is used per day and (5) number of hours the computer is locked per day. In the remainder of this thesis, when referring to locks per hour worked, it is de facto the number of hours the computer has been logged on, subtracted by the number of hours the computer was locked.

Table 4.12. SL: Distribution of average pure working time per treatment group and period

Group	Average pure working time per day per PC			
	<i>Pre-test</i>	<i>Intervention</i>	<i>Short-term post- test</i>	<i>Long-term post-test</i>
Control group	5,058	4,951	4,962	5,080
Information provision	5,162	5,133	5,080	5,194
Salient reminder	5,179	5,066	5,126	5,177
Combined treatment	5,197	4,993	4,966	5,084
<i>Average</i>	<i>5,149</i>	<i>5,041</i>	<i>5,034</i>	<i>5,136</i>

4.2.2 Manual locks per hour worked

At first we looked at the effect of our treatments on manual locks per hour worked. That means whether employees actively locked their screen or not. It is irrelevant by how this has been done. This could either be done by; (1) our suggested hotkey combination windows logo + L; (2) by clicking on start and then on lock; (3) by using the ctrl + alt + del hotkey combination etc..

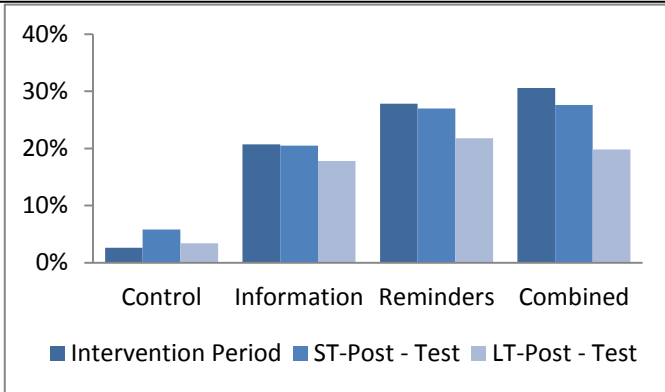


Figure 4.7. SL: Percentage increase of manual locks per hour worked, compared to the pre-test period.

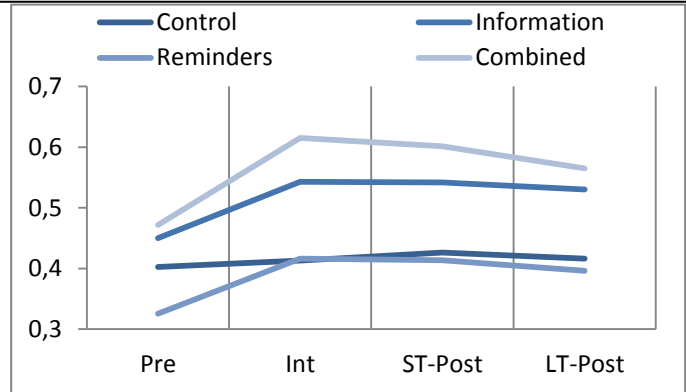


Figure 4.8. SL: Absolute change of manual locks per hour worked, per period.

A first glance at *Figure 4.8* and *Table 4.12* shows large baseline differences of manual locks per hour worked, between the four groups. Therefore and due to convenience reasons, we look at relative (percentage) changes- instead of absolute (numeric values). The number of manual locks per hour worked is, for all three treatments, higher in the intervention period compared to the pre-test period ($P < 0,001$). Moreover, the effect of treatments in all three treatment groups, remained two weeks after treatments were stopped (short-term post-test period) ($P < 0,001$). Although slightly diminished, the number of manual locks per hour is still higher two months after treatments were stopped (long-term post-test period), compared to the pre-test period. For all three treatments, this increase is statistically significant ($p < 0,01$).

Table 4.13. SL: Summary statistics. Mean and Standard deviation of number of manual locks per hour worked, and (average used) Pc's per treatment group.

Group	PC's	Average used PC's	Manual locks per hour worked							
			P1*		P2		P3		P4	
			M	SD	M	SD	M	SD	M	SD
Control group	523	346	0,403	0,701	0,413	0,694	0,426	0,687	0,416	0,663
Information provision	472	322,9	0,450	0,697	0,543	0,763	0,542	0,749	0,530	0,725
Salient reminders	484	319,4	0,326	0,580	0,416	0,660	0,413	0,673	0,396	0,561
Combined treatment	535	341,9	0,471	0,727	0,615	0,908	0,602	0,867	0,565	0,785
<i>Average</i>	<i>503,5</i>	<i>332,55</i>	<i>0,417</i>		<i>0,503</i>		<i>0,501</i>		<i>0,483</i>	

*P1 = Period 1 (Pre-test), P2= Intervention period, P3= Short-term post-test (two weeks after treatments were stopped) and P4= Long-term post-test period (two months after treatments were stopped)

For all period comparisons (pre-test, intervention period, short-term post-test and long-term post-test), the number of times participants manually locked their screens is not significantly different in the control group ($p < 0,05$) (*Table 4.13* & *Appendix 4.10*). The number of manually locks increased with 2,60% in the intervention period, 5,82% in the short-term post-test period, and 3,43% in the long-term post-test period. Differences although, are statistically insignificant ($p > 0,05$) (*Appendix A.4.12*).

Providing information significantly increased the number of times participants manually locked their screens (pre-test: $M=0,450$; $SD=0,697$, intervention period: $M=0,543$; $SD=0,763$, $t=-6.236$; $P<0,001$). Compared to the pre-test period, treatment effects remained two weeks (pre-test: $M=0,450$; $SD=0,697$, short-term post-test: $M=0,542$; $SD=0,749$, $t=-6,197$; $P<0,001$) and two months after treatments were stopped (pre-test: $M=0,450$; $SD=0,697$, long-term post-test: $M=0,530$; $SD=0,725$, $t=-5,535$; $P<0,001$). The number of manually locks increased with respectively 20,69% (Intervention period), 20,48% (short-term post-test) and 17,82% (long-term post-test), compared to the pre-test period. The number of times participants manually locked their screens is not significantly ($p>0,05$) different in period comparisons between intervention period, and two weeks (short-term post-test) -and two months after treatments were stopped (long-term post-test)(Appendix 4.12.).

Table 4.14. SL: T- test results, Number of times of manually locked screens, Intervention Period, Short-term post-test and Long-term post-test compared to pre-test period, per treatment group,

Group	Period 1 – Period 2	Period 1 – Period 3	Period 1 – Period 4
Control	$t=-0.663$; $P= 0.507$	$t=-1.488$; $P= 0.137$	$t=-0.895$; $P= 0.371$
Information	$t=-6.236$; $P= 0.000$ ***	$t=-6.197$; $P= 0.000$ ***	$t=-5.535$; $P= 0.000$ ***
Reminders	$t=-5.934$; $P= 0.000$ ***	$t=-5.723$; $P= 0.000$ ***	$t=-5.101$; $P= 0.000$ ***
Combined	$t=-7,625$; $P= 0.000$ ***	$t=-7.116$; $P= 0.000$ ***	$t=-5.394$; $P= 0.000$ ***

* $P<0,10$, ** $P<0,05$, *** $P<0,01$

Furthermore, (constant) salient reminders significantly increased the number of times participants manually locked their screens (pre-test: $M=0,326$; $SD=0,580$, intervention period: $M=0,416$; $SD=0,660$, $t=-5,934$; $P<0,001$). Compared to the pre-test period, treatment effects remained two weeks (pre-test: $M= 0,326$; $SD= 0,580$, short-term post-test: $M=0,413$; $SD=0,673$, $t=-6,197$; $P<0,001$) -and two months after treatments were stopped (pre-test: $M=0,326$; $SD=0,580$, long-term post-test: $M=0,396$; $SD=0,561$, $t=-5,101$; $P<0,001$). The number of manually locks increased with respectively 27,80% (Intervention period), 26,99% (short-term post-test) and 21,78% (long-term post-test), compared to the pre-test period. All three percentage increases are higher compared to the information provision treatment group. The number of times participants manually locked their screens is not significantly ($p>0,05$) different in period comparisons between intervention period, and two weeks (short-term post-test) -and two months after treatments were stopped (long-term post-test)(Appendix 4.12.).

Finally, the combined treatment significantly increased the number of times participants manually locked their screens (pre-test: $M=0,471$; $SD=0,727$, intervention period: $M=0,416$; $SD=0,660$, $t=-7,625$; $P<0,001$). Compared to the pre-test period, treatment effects remained two weeks (pre-test: $M=0,471$; $SD=0,727$, short-term post-test: $M=0,602$; $SD=0,867$, $t=-7,116$; $P<0,001$) -and two months after treatments were stopped(pre-test: $M=0,471$; $SD=0,727$, long-term post-test: $M=0,565$; $SD=0,785$, $t=-5,394$; $P<0,001$). In this group, the percentage increase of number of manually locks is the highest (compared to the information provision -and (constant) salient reminder treatment) in the intervention period (30,54%) and two weeks after treatments were

stopped (short-term post-test period=27,61%). The percentage increase in the two months after treatments were stopped (long-term post-test) is 19,82% (compared to the pre-test period). Therefore, as shown by *Figure 4.8* and *Table 4.12*, we observed two months after treatments were stopped (long-term post-test period) a significant decline in the number of times participants manually locked their screen, compared to the intervention period ($t=2,42$; $P=0,015$). The number of times participants manually locked their screen is also significantly lower two months after treatments were stopped (long-term post-test), compared to 2 weeks after treatments were stopped ((at a 10% significance level) ($t=1,812$; $P=0,070$)) (*Appendix 4.12.*).

4.2.3 Ratio of manual locks to total locks

Next to the fact that we were interested to see whether treatments are effective in increasing the number of manual locks per hour worked, we wanted to test, whether treatments also affect the ratio of manual locks to total locks (i.e. whether treatments would shift the percentage of manual locks of total locks upwards).

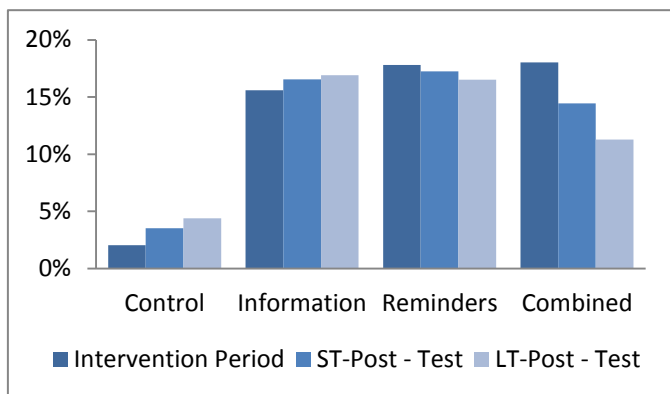


Figure 4.9. SL: Percentage increase of the ratio of manual locks to total locks, compared to the pre-test period.

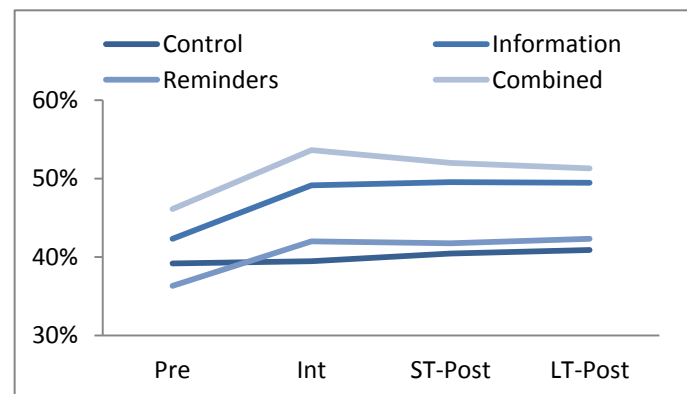


Figure 4.10. SL: Absolute change of the ratio of manual locks to total locks, per period.

As shown by *Figure 4.9* and *4.10* all treatments are effective in increasing the ratio of manual locks to total locks. As reported in *Table 4.15* and *4.16*, if comparing the pre-test period with the intervention period, and the periods two weeks (short-term post-test) –and two months after treatments were stopped (long-term post-test periods), all three treatments significantly increased the ratio of manual locks to total locks. Also, there are no significant differences between the intervention period, two weeks (short-term post-test) –and two months (long-term post-test period) after treatments were stopped, except the difference of the intervention period and two months after treatments were stopped in the combined treatment. Furthermore, for all period comparisons, differences in the control group are insignificant ($p>0,05$). However, the ratio of manual locks to total locks in the periods two weeks (short-term post-test) –and two months after treatments were stopped (long-term post-test), is significantly higher compared to the pre-test period at a 10 % significance level.

Table 4.15. SL: Summary statistics. Mean and Standard deviation of the ratio number of manual locks to total locks, per treatment group and period

Group	Ratio manual locks to total locks							
	<u>P1</u>		<u>P2</u>		<u>P3</u>		<u>P4</u>	
	M	SD	M	SD	M	SD	M	SD
Control	0,392	0,414	0,395	0,417	0,405	0,419	0,409	0,421
Information	0,423	0,419	0,492	0,423	0,495	0,425	0,495	0,425
Reminders	0,364	0,403	0,420	0,413	0,418	0,415	0,424	0,422
Combined	0,461	0,430	0,536	0,425	0,520	0,430	0,513	0,436
<u>Average</u>	<u>0,412</u>		<u>0,464</u>		<u>0,463</u>		<u>0,463</u>	

Comparing *Table 4.13.* & *4.14.* and *4.15.* & *4.16.* we found that findings of statistically differences between periods are in line with results of the treatment effectiveness on the number of manual locks per hour worked. This indicates that, compared to the pre-test period, information provision, make use of salient reminders and the combined treatment are effective in increasing the ratio of manual locks to total locks in the intervention period, and the periods two weeks (short-term post-test) –and two months after treatments were stopped (long-term post-test period. Means and standard deviations of all four groups –and periods are presented at *Table 4.15*). Contrary to findings presented in the previous section, the ratio of manual locks to total locks is not significantly different two weeks after treatments were stopped, compared with two months after treatments were stopped.

Table 4.16. SL: *t*-test results, ratio manual locks to total locks: Intervention, Short-term post-test and Long-term post-test period compared to pre-test period, per treatment group.

Group	Period 1 – Period 2	Period 1 – Period 3	Period 1 – Period 4
Control	t= -0,332; P= 0,740	t= -1,766; P= 0,078 *	t= -1,862; P= 0,060 *
Information	t= -8,188; P= 0,000 ***	t= -8,619; P= 0,000 ***	t= -8,549; P= 0,000 ***
Reminders	t= -5,888; P= 0,000 ***	t= -5,650; P= 0,000 ***	t= -6,137; P= 0,000 ***
Combined	t= -7,982; P= 0,000 ***	t= -6,227; P= 0,000 ***	t= -5,409; P= 0,000 ***

*P<0,10, **P<0,05, *** P<0,01

4.2.4 Regression Analysis

To explore factors that have an effect on screen locking behaviour, we performed fixed- and random effects panel data regressions. This section explains the steps we took to build the model and discusses the results from our regressions. We included in our model, independent variables; (1) pure working time (in hours [zuiverewerktijdu], (2) Period & Group dummies [Per2G2 etc.](2) Day of the week [Mon-Fri], (3) period dummy [dperiod (1-4)], and (4) the fraction of used computer of total computers per hallway [usedpcoftotalpc]. We conducted a Hausman test,

whereby we reject the null hypothesis that the difference in the coefficients is not systematic. Therefore we reject that the Random Effects model is a consistent estimator model, so we used the Fixed Effects model (*Appendix 4.13.*: Main model: $\chi^2=151,76$; $P=0,000$, *Appendix 4.19.*: Extended model: $\chi^2=168,39$; $P=0,000$).

Furthermore we checked for heteroscedasticity and autocorrelation. Test results indicate both heteroscedasticity (Main model: $\chi(1,1812)=4,9e+06$; $P<0,001$, Extended model: $\chi(1812)=5,4e+06$; $P<0,001$) and autocorrelation (Main model: $F(1,1761)=22,735$; $P<0,001$, Extended model: $F(1,1761)=22,389$; $P<0,001$). Therefore we used Driscoll-Kraay robust standard errors, which produces standard errors that are robust to disturbances being heteroscedastic, autocorrelated and cross-sectionally dependent. Also it is suitable for use with highly unbalanced panels and can handle missing values (Hoechle, 2007; Vogelsang, 2012). Correlation matrices, variance inflation factor values and test statistics for heteroscedasticity and autocorrelation can be found in the following appendices; Main model: *Appendix 4.14.*, *4.15.* and *4.16.*, Extended model: *Appendix 4.20.*, *4.21.* and *4.22.*.

In the extended model we include interactions terms of our time variable (zuiverewerktijdu) and group and period dummies (Per2G2 etc. & Period(1-4)), so that we can observe the impact of the number of hours worked on treatment effects.

Model 1: Main model

In *Table 4.18* we report variables of our main and extended model. In the intervention period, all three treatments significantly increased the number of times participants manually locked their screens (T1¹⁰: $\beta=0,477$; $SD=0,070$, $t=6,82$; $p<0,001$. T2¹¹: $\beta=0,390$; $SD=0,034$, $t=11,57$; $p<0,001$. T3¹²: $\beta=0,664$; $SD=0,051$, $t=13,11$; $p<0,001$). The combined treatment (T3) reported to have the highest increase in participants manually locking their screen. The difference with only providing information (T1) or (constant) salient reminders (T2) is statistically significant (T3-T1: $F(1, 62751)=25,35$; $P=0,000$, T3-T2: $F(1,62751)=33,00$; $P=0,000$). The difference between the information provision treatment and the constant salient reminder treatment is not significant (T1-T2: $F(1, 62751)=1,58$; $P=0,215$) (*Table 4.17*).

Table 4.17. SL: Treatment impact comparison in the intervention period

	Salient reminders treatment	Combined treatment
Information treatment	$F= 1,58$; $P= 0,215$	$F= 25,35$; $P= 0,000$ ***
Salient reminders treatment		$F= 33,00$; $P= 0,000$ ***

* $P<0,10$, ** $P<0,05$, *** $P<0,01$

¹⁰ T1 = treatment 1, information provision treatment (A5-Flyers).

¹¹ T2 = treatment 2, (constant) salient reminders treatment (stickers).

¹² T3 = treatment 3, combined treatment of both information provision (A5-flyers) and (constant) salient reminders (stickers).

Table 4.18. SL: Y= Handlock (number of manual locks), Main and extended model. Fixed effects regression analysis with parameters and Driscoll-Kraay standard errors.

Description	Variable	Model 1		Model 2	
		β	SE	B	SE
<i>Period dummies</i>	dperiode2	0,013	0,040	-0,148 **	0,070
Periode2 = intervention	dperiode3	0,053	0,044	-0,131	0,078
Periode3 = short-term post-test	dperiode4	0,050	0,048	-0,021	0,129
Periode4 = long-term post-test					
<i>Period * group dummies</i>	Per2G2	0,477 ***	0,070	0,580 ***	0,193
G2= Information provision	Per2G3	0,390 ***	0,034	0,243 *	0,122
G3= Salient reminders	Per2G4	0,664 ***	0,051	0,454 ***	0,114
G4= Combined treatment	Per3G2	0,377 ***	0,098	0,449 **	0,179
	Per3G3	0,371 ***	0,053	0,496 ***	0,143
	Per3G4	0,518 ***	0,070	0,204	0,203
	Per4G2	0,343 ***	0,086	0,418 **	0,165
	Per4G3	0,326 ***	0,061	0,244 **	0,114
	Per4G4	0,402 ***	0,061	0,192	0,132
<i>Working hours</i>	zuiverewerktijdu	0,035 ***	0,011	0,014	0,017
<i>Day of the week</i>	Tuesday	-0,023	0,027	-0,025	0,026
	Wednesday	-0,110 ***	0,037	-0,110 ***	0,037
	Thursday	0,007	0,045	-0,006	0,045
	Friday	-0,377 ***	0,058	-0,376 ***	0,058
<i>Fraction of used computers</i>	usedpcoftotalpc	0,831 ***	0,184	0,840 ***	0,017
<i>Interaction term</i>	G2Time			0,044 **	0,017
<i>Group * Time</i>	G3Time			-0,066 ***	0,019
	G4Time			-0,005	0,022
<i>Interaction term</i>	Per2Time			0,032 *	0,016
<i>Period * Time</i>	Per3Time			0,036 *	0,019
	Per4Time			0,014	0,026
<i>Interaction terms</i>	Per2G2Time			-0,020	0,030
<i>Period * group * time</i>	Per2G3Time			-0,026	0,020
	Per2G4Time			-0,041	0,025

Per3G2Time	-0,014	0,026
Per3G3Time	-0,025	0,027
Per3G4Time	0,062	0,042
Per4GTime	-0,015	0,023
Per4G3Time	0,015	0,022
Per4G4Time	0,040	0,027

*P<0,1 ** p<0,05 *** p<0,01

Furthermore, we analysed whether the effect of treatments would remain when they were stopped. Therefore we look at the variables in the third period, two weeks after treatments were stopped (short-term post-test). Compared to the pre-test period and control group, for all three treatments, the impact of treatments remained after treatments were stopped. All three treatments still significantly increased the number of times participants manually locked their screens (T1: $\beta=0,377$; $SD=0,098$, $t=3,86$; $P<0,001$. T2: $\beta=0,371$; $SD=0,053$, $t=7,04$; $P<0,001$. T3: $\beta=0,518$; $SD=0,070$, $t=7,41$; $P<0,001$). In line with findings in the intervention period, the number of times participants manually locked their screens is significantly higher in the combined treatment, compared to the information provision treatment ($F(1,62751)=9,54$; $P=0,004$) and (constant) salient reminder treatment ($F(1,62751)=8,24$; $P=0,006$). The difference between the information provision treatment and constant salient reminder treatment is not significant (T1-T2: $F(1,62751)=0,01$; $P=0,928$) (Table 4.18.).

Table 4.19. SL: Treatment impact comparison two weeks after treatments were stopped (short-term post-test)

Main model	Salient reminders treatment	Combined treatment
Information treatment	$F= 0,01$; $P= 0,928$	$F= 9,54$; $P= 0,004$ ***
Salient reminders treatment		$F= 8,24$; $P= 0,006$ ***

*P<0,10, **P<0,05, *** P<0,01

Also providing information, making use of (constant) salient reminders and the combination of these two treatments, significantly increased the number of manually locked screens, even two months after treatments are stopped (long-term post-test period)(T1: $\beta=0,343$; $SD=0,086$, $t=3,98$; $P<0,001$. T2: $\beta=0,326$; $SD=0,061$, $t=5,29$; $P<0,001$. T3: $\beta=0,402$; $SD=0,061$, $t=6,61$; $P<0,001$). The number of times participants manually locked their screens is on average +- 0,4 times higher in all three treatment categories, compared to the control group and pre-test period. Contrary to the findings of the intervention and short-term post test period, differences between the combined treatment and information provision treatment and (constant) salient reminder treatment are not significant (T3-T1: $F(1, 62751)=1,59$; $P=0,214$, T3-T2: $F(1, 62751)=1,06$; $P=0,308$). Differences between the information provision treatment and constant salient reminder treatment are also insignificant (T1-T2: ($F(1, 62751)=0,03$; $P=0,853$) (Table 4.19).

Table 4.20. SL: Treatment impact comparison two months after treatments were stopped (long-term post-test)

Main model	Salient reminders treatment	Combined treatment
Information treatment	F= 0,03; P= 0,853	F= 1,59; P= 0,214
Salient reminders treatment		F= 1,06; P= 0,308

*P<0,10, **P<0,05, *** P<0,01

Moreover, the impact of treatments does not change over time (e.g. comparing the intervention period with the short-term and long-term post-test period), for participants in the (constant) salient reminder treatment. However, in both the information provision treatment and the combined treatment, the number of times participants manually locked their screen is significantly lower two months after treatments were stopped (long-term post-test) compared to the intervention period (Information provision treatment: $F(1,62751)=6,05$; $P=0,018$, Combined treatment: $F(1,58613)=29,93$; $P=0,000$). Furthermore, in the combined treatment, the number of times participants manually locked their screen is significantly lower two weeks after treatments were stopped, compared to the intervention period ($F(1,58613)=6,27$; $P=0,016$). All other period comparisons are insignificant ($p>0,05$) (Table 4.20.).

Table 4.21. SL: Treatment impact comparison of Per2-Per3, Per2-Per4 and Per3-Per4 – Main model

Group	Period 2 ¹³ – Period 3 ¹⁴	Period 2 – Period 4 ¹⁵	Period 3 – Period 4
Information	F= 1,57; P= 0,217	F= 6,05; P= 0,018 **	F= 0,19; P= 0,690
Reminders	F= 0,09; P= 0,760	F= 0,85; P= 0,361	F= 0,30; P= 0,587
Combined	F= 6,27; P= 0,016 **	F=29,93; P= 0,000 ***	F= 3,35; P= 0,074

*P<0,10, **P<0,05, *** P<0,01

Finally, an increase in pure working time, increased the number of times participants manually locked their screens ($\beta=0,035$; $SD=0,011$, $t=3,33$; $P=0,002$). Compared to Mondays, participants working on Wednesdays and Fridays, significantly manually locked their screen fewer (Wed: $\beta=-0,110$; $SD=0,005$, $t=-2,96$; $p=0,005$. Fri: $\beta=-0,377$; $SD=0,058$, $t=-6,48$; $P<0,001$). Working on Tuesdays and Thursdays, does not significantly in-or decrease the number of times participants manually locked their screens ($p>0,05$). Also the percentage of occupied computers of total computers per hallway is positively related to the number of times participants manually locked their screens ($\beta=0,832$; $SD=0,184$, $t=4,53$; $P<0,001$).

¹³ Period 2 = intervention period

¹⁴ Period 3 = two weeks after treatments were stopped (short-term post-test)

¹⁵ Period 4 = two months after treatments were stopped (long-term post-test)

Model 2: Extended model with time interaction terms

We have extended our main model, by including interaction terms of pure working time (hours worked), period and group dummies. This allowed us to observe the impact of hours worked on the impact of treatment effects, periods and groups. In line with results of our first model, all treatment groups have a positive impact on the number of times participants lock their screens in the intervention period, and the periods two weeks (short-term post-test) –and two months after treatments were stopped (long-term post-test). To measure the impact of treatment effectiveness, we took the multiplied interaction term of time and group periodic dummies with the average hours worked per group and period, and added the coefficients of periodic group dummies (for example; impact of treatment 1 in period2 = ((Average time G2P2 * Per2G2Time) + Per2G2)).

We then constructed Wald-tests to test whether treatment effects are equal to zero, and state that all treatments in the intervention period, and the periods two weeks (short-term post-test) –and two months after treatments were stopped (long-term post-test period) significantly increased the number of times participants manually locked their screen ($P < 0,001$). Moreover we constructed Wald-tests to test differences in effectiveness of treatments.

Table 4.22. SL: Treatment impact comparison in the intervention period

Extended model	Salient reminders treatment	Combined treatment
Information treatment	F= 1,61; P= 0,212	F= 19,15; P= 0,000 ***
Salient reminders treatment		F= 32,05; P= 0,000 ***

* $P < 0,10$, ** $P < 0,05$, *** $P < 0,01$

In line with findings of the main model, in the intervention period, the number of times participants manually locked their screens is significantly higher in the combined treatment, compared to the information provision treatment ($F(1,62571)=19,15$; $P=0,000$) and the (constant) salient reminder treatment ($F(1,62571)=32,05$; $P=0,000$). The difference between the information provision treatment and (constant) salient reminder treatment is not significant ($T1-T2$: $F(1, 62571)=1,61$; $P=0,212$). The same holds for results in the short-term post-test period, whereas participants in the combined treatment significantly locked their screens more, compared to the information provision treatment ($T1$ ($F(1, 62571)=7,06$; $P=0,011$) and the (constant) salient reminder treatment ($F(1, 62571)=7,47$; $P=0,009$). The difference between the information provision treatment and the (constant) salient reminder treatment is not significant ($T1-T2$: $F(1, 62571)=0,02$; $P=0,883$) (Table 4.22.).

Table 4.23. SL: Treatment impact comparison two weeks after treatments were stopped (short-term post-test)

Extended model	Salient reminders treatment	Combined treatment
Information treatment	F= 0,02; P= 0,883	F= 7,06; P= 0,011 **
Salient reminders treatment		F= 7,47; P= 0,009 ***

* $P < 0,10$, ** $P < 0,05$, *** $P < 0,01$

Furthermore, in the long-term post-test period, participants in no treatment group, manually locked their screen significantly more or less. Although, compared to the control group, in all three treatment groups, the number of times participants manually locked their screen is significantly higher (T1-T2: $F(1, 62571)=0,03$; $P=0,858$, T1-T3: $F(1, 62571)=1,28$; $P=0,264$, and T2-T3: $F(1, 62571)=0,86$; $P=0,359$) (Table 4.23.).

Table 4.24. SL: Treatment impact comparison in the long-term post-test period

Extended model	Salient reminders treatment	Combined treatment
Information treatment	$F= 0,03$; $P= 0,858$	$F= 1,26$; $P= 0,264$
Salient reminders treatment		$F= 0,86$; $P= 0,359$

* $P<0,10$, ** $P<0,05$, *** $P<0,01$

As shown in Table 4.24., in line with findings of the main model, the impact of treatments does not change over time for participants in the (constant) salient reminder treatment. Both the information provision treatment and the combined treatment, the number of times participants manually locked their screen is significantly lower two months after treatments were stopped (long-term post-test) compared to the intervention period. Also, in the combined treatment, the number of times participants manually locked their screen is significantly lower two weeks after treatments were stopped, compared to the intervention period all other period comparisons are insignificant ($p>0,05$).

Table 4.25. SL: Treatment impact comparison of Per2-Per3, Per2-Per and Per3-Per4 – Extended model

Group	Period 2 – Period 3	Period 2 – Period 4	Period 3 – Period 4
Information	$F= 1,45$; $P= 0,235$	$F= 5,93$; $P= 0,019$ **	$F= 0,21$; $P= 0,649$
Reminders	$F= 0,03$; $P= 0,867$	$F= 0,54$; $P= 0,467$	$F= 0,23$; $P= 0,634$
Combined	$F= 6,93$; $P= 0,012$ **	$F= 30,70$; $P= 0,000$ ***	$F= 3,57$; $P= 0,065$

* $P<0,10$, ** $P<0,05$, *** $P<0,01$

Moreover, an important observation is that treatment effects are not significantly affected by time (e.g. interaction effects of treatment with time are insignificant ($p>0,05$)). However, we do observe significant effects of time on (treatment) groups. Whereas time has an overall positive effect on the number participants manually lock their screen for participants in group 2, the information provision treatment ($\beta=0,031$; $SD=0,016$, $t=2,64$; $P=0,011$), the effect of time is negatively related to group 3, the (constant) salient reminder treatment ($\beta=-0,066$; $SD=0,019$, $t=-3,49$; $P=0,001$). The effect of time on participants in the combined treatment is insignificant ($p>0,05$).

Furthermore, a notable finding is that in the extended model the period dummy for the intervention period, become significant and negative ($P < 0,05$). Although the interaction term with working hours is positive, it indicates that if participants work less than 4,69 hours, compared to the pre-test, the number of times computers are manually locked decreases ($P < 0,05$). However, as shown in *Appendix 4.11.*, the average hours pure working time is 5,04, so the impact of time on the intervention period on the behaviour of participants who has an average working time a day is positive related to the number of times participants manually locked their screen. In the short-term post-test period, time also has a positive effect on the number of times participants locked their screen if average working time a day is above 3,62 hours, whereas the average is 5,034 hours. Results are in line with findings as shown in the main model, which also indicates a positive relationship of the intervention period and short-term post-test period on the number of times participants manually locked their screen, although insignificant ($p > 0,05$).

Last, although the effect is insignificant, an increase in pure working time, increased the number of times participants manually locked their screens ($\beta = 0,014$; $SD = 0,017$, $t = 0,80$; $P > 0,05$). Compared to Mondays, participants working on Wednesdays and Fridays, significantly manually locked their screen less (Wed: $\beta = -0,111$; $SD = 0,037$, $t = -2,98$; $p = 0,005$. Fri: $\beta = -0,376$; $SD = 0,058$, $t = -6,54$; $P < 0,001$). Working on Tuesdays and Thursdays, does not significantly in-or decrease the number of times participants manually locked their screens ($p > 0,05$). Also the percentage of occupied computers of total computers per hallway is positively related to the number of times participants manually locked their screens ($\beta = 0,840$; $SD = 0,182$, $t = 4,60$; $P < 0,001$).

Chapter 5: Discussion

In this study we tested the extent to which security education, training and awareness programs can contribute to effectively promote information secure behaviour in an organizational context. This relationship is analysed by two field experiments (phishing and screen locking) in which several interventions were tested. We found that in both of our experiments all three treatments are effective in promoting information secure behaviour, compared to the control group. In the remainder of this chapter we will refer to our research questions and hypotheses, and compare our findings with other studies.

Main Question: How can information secure behaviour be effectively promoted in an organizational context?

5.1 Phishing

In comparison with the control group, both the percentage of participants who clicked on the link embedded in the phishing email, and who filled in passwords, is significantly lower in all three treatment groups. This study therefore contributes to the growing field of how behavioural insights can be applied to improve information secure behaviour. Although, some of the findings presented in this study are in contradiction with other studies, most interesting is to see, which elements of training materials are more or less effective than others. At first we will discuss our findings regarding our first measurement, the percentage of participant who visited the site.

5.1.1 Measurement 1: Participants clicked on the link

Compared to the control group, all three treatments significantly reduced participants likelihood of clicking on the link embedded in the phishing email. Comparing the effectiveness of treatments, we found that simulating previous experience with phishing mails was more effective than providing information. Simulating previous experience with phishing mails and providing information is not more effective than solely providing information or solely simulating experience with phishing emails. It even turned out that solely simulating previous experience was more effective then combining the simulation of previous experience and the provision of information. Furthermore, men and employees with an internal employment contract were more likely to click on the link embedded in the phishing mail, compared to females and to those with an external contract. Also compared to participants aged 16-25, the higher age, the more participants were likely to click on the link embedded in the phishing mail. However, the likelihood decreases if age is larger than 55.

5.1.2 Measurement 2: Participants filled in passwords

Furthermore with respect to the second measurement, all three treatments also significantly reduced participants' likelihood of filling in passwords. Moreover, the two treatments, in which previous experience was simulated (simulating experience treatment and combined treatment), were more effective than the information provision treatment. Simulating previous experience with phishing emails and providing information was not more effective than only simulating previous experience with phishing emails. Contrary to findings regarding the likelihood participants clicked on the link embedded in the phishing email, no significant effects were found for gender and employee contract. Last, compared to participants aged 16-25, there are no significant differences with age categories for participants aged 26-35 and aged 36-45. However, participants aged 46-55 and 55+ were more likely to fill in passwords.

5.1.3 General discussion

In chapter two we have described the most relevant factors affecting someone's susceptibility towards phishing fraud; (1) limited attention to incoming mails, (2) lack of knowledge and experience, and (3) distributed responsibility and low risk perception. In order to mitigate the influence of such factors, previous studies have tested different elements of training and education. However, differences of effectiveness were found in studies, which make it less clear, which elements are effective in reducing someone's susceptibility to phishing fraud. Furthermore, ambiguity of effective interventions is enhanced by differences in experimental setup. Since most studies involved role-play activities or took place in a university setting, results could be different due to population and/or observer-expectancy bias.

In this study we have tested effectiveness of interventions in an organizational context, with complete waiver of consent. Therefore, we were able to approach the situation of a received phishing email as realistic as possible, allowing us to observe actual behaviour which was not affected by experimental biases. We proposed an intervention strategy to test effectiveness of information provision (infographics by mail) and/or simulating previous experience with phishing emails, of which both interventions taught people about phishing during their normal use of email. *Table 5.1* provides an overview of fully, partially and not supported hypotheses.

Table 5.1. *PM:* Susceptibility towards phishing fraud – fully, partially and not- supported hypotheses

Hypothesis	Effect	Description	Supported
H1A	-	Information provision reduces	Fully
H1B	-	Previous experience reduces	Fully
H1C	--	Combined treatment is most effective	Not
H2A	+	Age	Not
H2B	-	No gender effect	Partially ¹
H2C	+	Internal employee	Fully

¹ Males visited the site significantly more, compared to females. We found no significant gender effect regarding the percentage of participants filling in their password.

RQ1: What treatments are effective in reducing participants' susceptibility to phishing email fraud?

As mentioned in chapter 2, literature has shown ambiguous results for the effectiveness of communication strategies in order to prevent people from becoming victim of phishing fraud. The ambiguity of effectiveness can be explained by differences in which- and how information is provided. For example, effectiveness of communication can be enhanced, by incorporating both fear appeals and effective coping strategies (David & Sillence, 2010).

In our first field experiment we found information provision (H1A) to be effective in reducing both the percentage of participants clicking on the link embedded in the phishing mail, as the percentage of participants who filled in their password. Although we believe the content (coping strategy) of the infographics was of high importance, we also made use of findings in support of the impact of style and visceral influences, on the effectiveness of communication (McCormac, 2015).

Therefore this thesis supports findings of Sheng et al. (2010) and Burns et al. (2013), who found that information provision based on text and images being simple and visually salient, are effective in reducing susceptibility to phishing fraud. Furthermore, it could enrich conclusions drawn by Kumaraguru et al. (2007), who found that risk communication alone, is not effective in decreasing susceptibility towards phishing fraud. They indicated that information should not only increase alertness, but also should educate participants about detection strategies. However, no distinction in this thesis was made in different forms of information provision, so no support can be given that the inclusion of fear appeals, coping strategies or both were of influence on the impact of our information provision treatment.

Moreover, simulating experience with phishing emails is more effective than providing information, in reducing participants' susceptibility to phishing fraud. This holds for both the percentage of participants who clicked on the embedded link in the phishing email, as the percentage of participants who filled in their password. However, when previous experience is combined with information provision in a treatment, treatment effectiveness is ambiguous compared to other treatments. Whereas, compared to information provision the combined treatment is more effective in reducing participants' likelihood to fill in their password, this does not hold for the likelihood of clicking on the embedded link in the phishing mail. One surprising finding was that participants in the combined treatment were even more likely to click on the link embedded in the phishing email, compared to those in the solely simulating previous experience treatment. Therefore we reject that the combined treatment is most effective in reducing participants' susceptibility to phishing fraud. Findings are in opposite of results from Bowen et al. (2011) and Burns et al. (2013), who found giving information after participants received a phishing email, to increase effectiveness. As explanation they propose that the mail had increased relevance of the provided information and therefore had higher impact. In our study however, we did not find such increased impact.

As previous studies have discussed several explanations of what causes previous experience to be effective, we try to contribute by giving ours. At the same time we try to explain why the combined treatment is more effective than information provision in reducing likelihood of filling in passwords, even though there is no difference in percentage of participants who clicked on the embedded link.

Whereas some propose the effectiveness of simulating previous experience it is due to increased self-efficacy (i.e. acquiring the necessary skills to recognize and report)(Siponen et al., 2014; Kumaraguru, 2009), others ascribe importance to altered risk perceptions and increased alertness. Of which the latter implies increased attention paid to incoming emails- and suspiciousness towards filling in personal details (Vishwanath et al., 2014).

In our experiment participants could detect the phishing scam in two stages. At first, participants can detect the mail as being fraudulent, based on knowledge and paid attention to recognizable cues of phishing. If participants recognize the mail as being fraudulent, they do not click on the link embedded in the phishing email, and therefore automatically also do not fill in personal details at the 'fake' website. Second, participants can detect phishing when they visit the 'fake' website, at which they were asked to fill in personal details. If participants recognize the website as being fraudulent, they do not fill in personal details.

We believe, that effectiveness of simulating previous experience with phishing fraud is related to obtaining higher familiarization with both stages of the phishing scam. On the one hand, this resulted in fewer participants clicking on the link embedded in the phishing email (first detection stage), as results of the simulated experience treatment indicated. On the other hand, this resulted in fewer participants who filled in their password (the second detection stage), as results of both the simulated experience treatment as the combined treatment indicated. Moreover, in the combined treatment the percentage of participants who filled in their password after they have clicked on the link embedded in the phishing email, is lower compared to those in the information provision treatment.

The redirection to the site (the second stage), where participants must fill in personal details could have raised red flags for those who had received a similar mail in advance. Although the participants who only received information were told that organizations would never ask for personal details (such that if they receive such request they must deny it), they had no experience with the whole phishing scam (i.e. what happened if they clicked on an 'infected' link). Therefore, although differences between the information provision treatment and the combined treatment of the likelihood participants clicked on the embedded link are insignificant, familiarization with both stages of phishing fraud reduced the likelihood participants filled in their password. This statement is supported by Sheng et al. (2007) who found that training techniques which include the demonstration of phishing emails and websites (both detection stages), to be more effective in increasing knowledge and techniques they can use to identify phishing scam.

RQ2A: What demographic factors affect someone's likelihood to fall for phishing email attacks.

To continue, we have examined the effect of gender and age on someone's likelihood to fall for phishing fraud. Overall the average age of participants falling for phishing fraud is 2 to 3 years above the average age of all participants. Furthermore we found that the compared to the reference category (16-25), the likelihood of clicking on the link embedded in the phishing email increased for age categories aged 36-45, 46-55 and 55+. This also holds for participants who filled in their passwords for the age categories aged 46-55, and 55+, and indicates that the higher age groups are more susceptible to phishing fraud. Findings therefore are contrary to those of Sheng et al. (2010) and Kumaraguru et al. (2009), who found that participants aged 18-25 are most likely to fall for phishing. However we believe, that (some of the) differences in results, can be explained by the differences in samples, since in both studies average age was more than 15 years lower compared to our sample.

Moreover, we found ambiguous gender effects, since men were more likely to click on the embedded link in the phishing mail, but were not more likely to fill in their passwords. Therefore we (partially) reject hypothesis H2B. Findings are in line of those of Kumaraguru et al. (2009) and Dhamija et al. (2006), but contrary to those of Jagatic et al. (2007), Sheng et al. (2010) and Kumaraguru et al. (2007), who found that females are more likely to fall for phishing attacks. However we believe, gender (even as age) not to be that important factor towards phishing susceptibility, since there could be posed dozens of underlying factors captured by the gender (and/or age) effect (e.g. job description, web experience, personal experience etc.). More relevant is that this study has identified particular subject groups who showed to be significantly more susceptible to phishing fraud than others. For example, this enables to provide tailor made trainings (materials) for those at highest risk.

RQ2B: How does the type of employment contract (external/ internal) affect susceptibility to phishing email fraud?

At last we have examined differences in employment contract (external/internal) affecting susceptibility to phishing fraud. We found internal employee to be more likely to fall for phishing fraud, compared to external (H2C). An explanation is given by Vishwanath et al. (2011), who stated that individuals' likelihood to respond to phishing emails is negatively related to the perceived relevance of particular messages. Especially the second phishing mail stated that employees had to increase their e-mail storage limit to make sure the account was not closed, could be extremely relevant for those for whom e-mail is vital for day-to-day tasks. We expect the perceived necessity of fast respond to be lower for external (who work on average less hours per week for the ministry) compared to internal employees. Findings of Vishwanath et al. (2011) are supported by Jagatic et al. (2007) stating that the social content of attacks may lead people to overlook important cues, lowering the guard and thereby making themselves more vulnerable to phishing fraud. Finally, since external employees work less, it could be simply due to the fact that fewer external employees had read the received phishing email, before the debriefing was send. Differences between organizational units were small, and not much scientific relevance can be attributed to those. However we reported those for practical relevance in the form of acquiring target groups for further and future training.

5.2 Screen locking

The second field experiment concerns more habitual behaviour and is perceived as low(er) risk. To our best knowledge, manually locking your screen has not yet been studied before. To improve compliance with screen locking procedures, we have tested effectiveness of three treatments; (1) information provision (handing out information flyers), (2) (constant) salient reminders (keyboard shortcuts where highlighted by green stickers), and (3) the combined treatment of both information provision and (constant) salient reminders. In comparison with the control group, the ratio of manual locks to total locks and the number of manual locks per hour worked is significantly higher in the treatment groups compared to the pre-test period. This holds for the intervention period and the periods two weeks (short-term post-test) –and two months (long-term post-test) after treatments were stopped. In the remainder of this chapter we continue our 'quest' of determining which elements of training are effective in promoting information secure behaviour.

5.2.1 Manual locks per hour & ratio manual locks to total locks

As shown in the previous chapter, both the number of manual locks per hour worked and the ratio of manual locks to total locks is, for all three treatments, higher in the intervention period, compared to the pre-test period. Furthermore, this does not count for the control group (remain constant over all the four periods). Moreover the effects of treatments remained in all three treatments groups two weeks after treatments are stopped (short-term post-test). Although slightly diminished, this also applies to the period two months after treatments were stopped (long-term post-test), compared to the pre-test period. Both types of measurement (for all three treatments) are not significantly different in period comparisons of the intervention period, and two weeks – and two months after treatments were stopped, except for the period comparison of the intervention period with the period two months after treatments were stopped, in the combined treatment.

Due to differences in baseline levels, we were only able to compare difference in results, rather than testing differences between treatments. Although, we can state that in the combined treatment group, the percentage increase in number of manually locks is the highest (compared to solely providing information or solely placing constant salient reminder on the keyboards) in the intervention period and two weeks after treatments were stopped. Comparing the pre-test period, with the period two months after treatments were stopped, the percentage increase is almost equal for all three treatments.

Results of the second measurement, the ratio of manual locks to total locks, showed that in the intervention period, the increase in percentages is almost equal among the three treatments. However, we observed a decline in percentage increase in the combined treatment group two weeks after treatments were stopped. Simultaneously, the percentage increase remains almost constant in the information provision treatment and the (constant) salient reminder treatment. A possible explanation is that the baseline level of the ratio of manual locks to total locks is up to 10% higher compared to other groups. This could indicate that an increase of the ratio of manual locks to total locks is harder to achieve for a higher baseline level, compared to a lower baseline.

5.2.2 Regression analysis

The constructed models, main and extended version, allowed us to explore the factors that had an effect on screen locking behaviour, and to test for differences in effectiveness of treatments. We found in both models, compared to the pre-test period, that all three treatments significantly increased the number of times participants manually locked their screen. This holds for the intervention period, and the periods two weeks- and two months after treatments were stopped. Moreover, both in the intervention period, as two weeks after treatments were stopped, the impact of treatment effect in the combined treatment, was higher compared to the other two treatments. We found same results in our extended model, when we took the average time (per group per period) participants worked per day. Therefore, in the intervention and two weeks after treatments were stopped, constant salient reminders and providing participants with information is more effective in than one of both. In the last period, two months after treatments were stopped, no treatment appears to be more effective than others. Although, for all three treatments, even two months after treatments were stopped the number of times participants manually locked their screen was higher, compared to the pre-test period.

Moreover, in both treatments in which participants were given information (flyers) (information provision –and combined treatment), the number of times participants manually locked their screen is significantly lower two months after treatments were stopped, compared to the intervention period. In the combined treatments, this also holds, when comparing the intervention period, with the period two weeks after treatments were stopped. Differences between the periods two weeks –and two months after treatments were stopped are insignificant, for all three treatments.

Furthermore we analysed the impact of time on the number of times participants manually locked their screen. Overall, in both models, an increase in hours worked per day increased the number of manually locks. The second (extended) model, allowed us to observe time specific effects. We found time to have a positive effect on participants in the information provision treatment, but a negative effect on those in the constant salient reminder treatment. Moreover, compared to Mondays, all other days of the workweek (Tue-Fri) have a negative impact on the number of times participants manually locked their screen. However only the impact of working on Wednesday's and Friday's is significant. Finally, the number of occupied pc's per hallway is positively related to the number of times participants manually locked their screen, indicating that an increase in occupied workstations per hallway, increased the number of manually locked screens.

5.2.3 General discussion

In our treatments, we have tried to enhance the 'right choice' of manually locking your screen by making use of constant salient reminders. Furthermore we have informed participants of why- and how you should lock your screen. When individuals do not see that they are truly confronted by IS security threats, they will have a less positive attitude towards protective behaviour (Herath & Rao 2009). Especially in an organizational context, protected by both physical and technical mechanisms, perceived risk of leaving your screen is very low. As posed by Adams (1983) protective mechanisms can even enhance risky behaviour. Another important reason for not locking your screen is 'high' perceived effort and hindrance, related to the protected environment. This combination alters the perceived relevance, and possibly the performance of information secure behaviour. However, as posed by Choi (2013) this could be mitigated by increasing computer-users knowledge (i.e. increasing self-efficacy of how to perform protective countermeasures). Moreover, behaviour is also influenced by those among us. Especially behaviour of superiors, but also of peers, is highly related to our perception of what right and accepted behaviour (Panko, 2012).

Table 5.2. SL: Number of times participants manually lock their screens - fully, partially and non- supported hypotheses

Hypothesis	Effect	Description	Supported
H3A	+	Information provision increases	Fully
H3B	+	Constant salient reminders increases	Fully
H3C	++	Combined treatment is most effective	Partially ¹
H4	+	Salient reminders are long-lasting effective	Partially ²
H5A	+	Ratio of used computers of total computers	Fully
H5B	+	number of hours worked	Partially

¹ It is most effective in the intervention period, and short-term post-test period, but not in the long-term post-test period.

² Compared to the control group, (constant) salient reminders are long-term effective. However, there are no differences in treatment effects in the long-term post-test, between all three treatments.

RQ3: What treatments are effective in improving manually locking your screen?

Results showed that information provision increased participants manually locking their screen, in the intervention period, and the periods two weeks- and two months after treatments were stopped (H3A). As mentioned in the discussion of our phishing mail experiment, literature showed ambiguous results of the effectiveness of information provision. Therefore we will elaborate a bit more on what we think, caused information provision to transfer information 'insecure' into more secure behaviour.

First, we did not only present participants with information about the presence of threats, but also, how one could mitigate and preferably eliminate the threats (i.e. we informed participants of the “why” and “how”) (David & Sillence, 2010). Another included, and common used strategy tool, is to incorporate social norms (Pahnila, 2007). Revealing the actual norm, to correct misperceptions will be beneficial for most individuals, who will either be encouraged to engage in protective behaviours or reduce their participation in potentially unsafe behaviour. Moreover, effectiveness of information provision can be enhanced by the fact that we placed the A5-flyers at the place where it was needed to be applied. Finally, we expect that since we redistributed flyers three times, the effect of reminding participants of the desired behaviour was of influence on effectiveness of the information intervention (Calzori & Nardotto, 2015).

Second, constant salient reminders had a positive effect on the number of times participants manually locked their screen, in the intervention period, and the periods two weeks- and two months after treatments were stopped (H3B). Results are in line with findings of Karlan et al. (2011), Calzolari & Nardotto, 2011) and Raifman et al. (2014), who found that reminders can have substantial impact on behaviour. One possible explanation is that the stimulus produced by reminders, focused the attention of the receiver towards the inflicted goal, and further away of many alternative goals. As proposed by Lewis & Eves (2011), by placing stickers on the keyboard of participants, we made the stimulus visible at the time behavioural choice was made. Attention thereby was driven to the desired behaviour, which in turn reminded employees to lock their screens.

Finally, in the intervention period and two weeks after treatments where stopped, the combined treatment of both constant salient reminders and information provision is most effective in increasing the number of times participants manually locked their screens (H3C). However, this does not hold for the period two months after treatments were stopped (long-term post-test). One explanation of why the combined treatment was most effective in the intervention period and the period two weeks after treatments were stopped, is that not only emphasizing desired behaviour, but also indicating why you should do so, enhances the effect of (constant) salient reminders. This explanation is in line with findings of Karlan et al. (2010) who found that reminders that highlighted its particular goal, were two times more effective than reminders that did not mention the goal. Another explanation is that some participants simply could not make the link between the reminders and its function. Information provision in this way, could contribute by stating clearly, why those keys on the keyboard were emphasized with green stickers. Although we had placed an extra sticker indicating the link between the stickers and the desired behaviour, some participants told to be unaware of the purpose of the stickers.

RQ4: Which treatments still have impact on screen locking behaviour, after treatments are stopped?

To analyse if treatments will lead to habit forming behaviour, we tested whether treatment effects remained after treatments were stopped. We separate this research question into two subsections, for the period two weeks –and two months after treatments were stopped.

As mentioned above, all three treatments remained its effectiveness two weeks after treatments have stopped. Furthermore, in this short-term post-test period, we found no differences in impact of treatments among those who received information and those with stickers. Although it is hard to mention it a lasting effect, we had not expected such results. However, some support was found in literature. A research conducted by Taubinsky (2013) found, the more a person had performed particular behaviour in the past, the more likely they are to be top of mind, and thus the more likely they are to be performed again. A possible explanation therefore could be that by informing participants of the likelihood to easily lock their screens with the keyboard shortcut, that the performed action became a repeated action, even after treatments were stopped. This line of reasoning could also be applied to constant salient reminders.

Furthermore, none of the three treatments had a larger or smaller impact on the number of times participants manually locked their screens, two months after treatments were stopped. However, for all treatments, the number of manual locks was higher compared to the pre-test period. We had anticipated, this would be the case for the treatments with constant salient reminders (constant salient reminder treatment and combined treatment), but not for the information provision treatment. One possible explanation could be that the time duration of two weeks intervention period, was too small to allow for permanently induced new, persistent habits, characterized by more frequent manual locks. Since the number of times participants manually locked their screen is still higher three months after treatments were stopped, some form of habit formation may have occurred.

Moreover, results of the regression analysis showed, that in both treatments in which participant were given information (flyers) (information provision –and combined treatment), the number of times participants manually locked their screen is lower two months after treatments were stopped, compared to the intervention period. Therefore, although information provision is effective in increasing the number of times participants manually locked their screen, two- weeks and two-months after treatments were stopped, treatment effectiveness declined. This does not apply to the treatment in which only (constant) salient reminders were used, which might indicate that (constant) salient reminders are more effective in generating persistent and improved behaviour over time. However, the question arises whether differences in treatment effectiveness among information provision and (constant) salient reminders will increase over time, or not.

RQ5: What is the effect of relative occupancy of workstations and number of hours worked on the number of times participants manually locked their screen?

Our next subject of interest was whether relative occupancy of workstation has an effect of information secure behaviour, regarding manually locking your screen. In other words, we wanted to test the effect of the ratio of occupied workstations to total of workstations per hallway, on the number of times participants manually locked their screen (H5A). We found the relative occupancy of workstations to be positively related, which can be explained by social influence. Pahanila et al. (2007) found that employees' perception of their peers and superior's complying with security policies were empirically significant predictors of employees' intentions to comply with information security standards. Therefore, by seeing others locking their screen it could enhance intentions to perform similar behaviour.

Finally, the number of hours worked is positively related to the number of times participants manually locked their screen (H5B). Furthermore time was positively related to the number of times participants manually locked their screen in the information provision treatment, and negatively related to those in the constant salient reminder treatment. Moreover time does not have a significant impact on specific treatments. Overall, the number of times participants manually locked their screen has a positive impact on participants who has an average working time a day, in the intervention period and two weeks after treatments were stopped.

5.3 Implications

This study contributes to the growing field of evidence of effective interventions which help individuals to behave more information secure, based on behavioural insights. Both for practitioners as scientist we believe this study has offered several contributions and implications. This counts for our phishing mail experiment and especially our screen lock experiment, because to our best knowledge, we were the first to explore this topic.

The most important findings are related to the effectiveness of different interventions. We found simulating previous experience with phishing fraud to be more effective, than simply informing individuals over phishing. Furthermore, the combined treatment of constant salient reminders and flyers was more effective than one of both, although there were no differences in the effectiveness of treatment two months after treatments were stopped. Moreover information provision treatment effectiveness declined over time, which does not apply to (constant) salient reminders. We believe findings have important implications for future design of intervention studies. Next to our main implication, we want to mention several other topics of which we believe that are important for both scientists as practitioners.

First, most studies have focused on high risk behaviour, such as phishing, or on the total of improvement of information secure behaviour. In this study we have also explored the field of more habitual behaviour, such as manually locking your screen, which by most employees is perceived as low(er) risk. We have determined relevant factors affecting individuals' behaviour regarding compliance with procedures of locking your screen, and were first to apply the effect of salience and reminders to the field of information security.

We found that relatively simple interventions can have large impact. Although perhaps simulating a phishing mail is not that easy, handing out flyers and placing stickers increased the number of manually locked computers up to +- 30 percent. Both turned out to be even effective up to two months later. Therefore with relative small effort and expenditures, large impact can be achieved. For both *practitioners* and *scientist*, results of the (constant) salient reminders intervention imply the wide applicability of salience and reminders, that we believe should also be applied to other domains.

Second, in our *phishing mail* experiment, we observed much more than simply the effectiveness of our interventions. The experiment, revealed among other things, strengths and weaknesses of the organization. For example, we noticed that many employees reacted alert, warned colleagues, and contacted IT support. Furthermore, from all directions employees started to ask for messages on intranet. Therefore such an experiment is perfectly suitable for *practitioners* to test the resilience of organizations against such threats, in the form of a "fire drill". Moreover, more than 80 percent of the participants who fall for phishing fraud, did so within three hours. Therefore, if organizations receive a phishing mail, an immediate action is required of both IT professionals as individual end-users. To facilitate a fast respond, knowledge and clear procedures of how to report phishing is of great importance. Finally, we have expanded the scope of subject populations in a university context, to the organizational context, and therefore showed the effectiveness of simulating previous experience with phishing emails to reduce the susceptibility of organizations. This is important, because vital assets of organizations are increasingly stored online and organizations are more and more dependent of computer systems. Therefore organizations are increasingly interesting for attackers, which means that organizations should devote more resources to protect themselves. We propose that simulating previous experience with phishing emails should be one of those. Results also indicated that giving information and simulating previous experience with phishing emails was not more effective than solely simulating previous experience, which should be taken into account by developing Security Education and Training and Awareness programs.

Third, although susceptibility to phishing fraud in all treatments decreased, we observed a large fraction that still fell for phishing fraud. Therefore for both *practitioners* and *scientists*, we imply that actions to increase information security should be an on-going topic of conversation, and that repeated actions are necessary to improve and maintain information secure behaviour. Although both experiments have illustrated its positive impact on information secure behaviour, they also indicated that there is certainly room left for improvement.

Fourth, in our *phishing mail* experiment we found, contrary to other studies, some demographics factors which could specify target groups at highest risk. *Scientifically* this is interesting, because further exploration of underlying facets could enrich conclusions of what drives someone to be more or less susceptible to phishing fraud. For *practitioners* this can give handful insights for developing tailor made training programs to create a better match of content and audience. However, one should always take into account that there can be many non-included factors what have driven this target group to stand out in our study.

Last, both experiments showed ambiguous results of the effectiveness of information provision. As discussed in previous literature, the impact of information provision is sometimes underestimated and sometimes overestimated. In our experiments we found information provision to reduce participants' susceptibility to phishing fraud, but was less effective compared to simulating experience with phishing emails. Furthermore, handing out flyers was effective in generating long-lasting treatment effects on the subject of manually locking your screen. Therefore we observed for different types of behaviour, differences in effectiveness of information provision. For example, we believe the higher impact of the latter can be explained by the fact that information was presented at the place and time where it was needed to be applied. Therefore for both *practitioners* and *scientists*, this implies that in order for information provision to be effective, one should consider several things. First, one should determine which factors influence the specific behaviour. Second, at what time -and place it is best to be presented. Third how- and which information should be presented (visceral influences, social norms, images etc.).

5.4 Limitations

Our study has some limitations. *First*, the data was obtained from one organization, which may include bias unique to the sample. Therefore, care should be taken in generalizing findings to other organizations. Furthermore in our screen locking experiment, we only looked at one particular building. Possibly, unique characteristics (i.e. small or large building, protective mechanisms such as entrance control etc.) could be of influence on our findings, which might be different if generalized to other buildings. *Second*, due to time constraints, our intervention period in the screen lock experiment took only two weeks, which is short compared to most studies adding to the framework of the effect of salient reminders. This could have an impact on our findings of the effect of salient reminders in the long-run. *Third*, also related to our screen locking experiment, different interventions took place in the same building. Since officially workplaces are flexible, participants could have been exposed to more than one condition. This also implies that findings are not unique participants based, but computer based. Therefore we could not fully eliminate the possibility of intervention spill over effects. However, we believed that this effect is limited due to our smart design of group formation and because we found no significant increase in the control group. However, the possibility of spill over effects should be taken into consideration. *Fourth*, we could not measure whether the increase in the number of manual locks was due to an increase of participants using our suggested hotkey, or that it increased the general tendency of locking your screen. Although it is for practical relevance not necessary to be made such distinction, this could be non-optimal for scientific relevance.

Fifth, regarding our *phishing experiment*, we only measured the number of participants who received the infographics and/or phishing emails, but not the number of participants who actually had read them. Although analyses of out of offices notices and standard replies, showed small differences between groups, we have no indication of the absolute number of participants who have actually read them. *Sixth*, as expected, after receiving the phishing email, some participant started warning others. This was done both in person and by making use of for example divisional mailing lists. Possibly, some received these warnings before the phishing mail was read, which disrupted the experience and assessment of the email. Although it was anticipated, we do not know

if such disruptions were equal among groups. Seventh, the study only tested a limited number of (similar) phishing mails. Both mails we tested, had resemblance in the relevance, length, recognizable cues, and required an immediate action of the receiver. Other mails, such as those related to social media, banking information and debt collection agencies, might result in different deception rates. Therefore we propose in order to generalize findings, one should also consider the possible impact of less similar and third party senders on differences in deception rates. However, due to two reasons we expect our choices of phishing mail resemblance and topics are justified. First, we have not opted for a third party sender, since legal issues requires consent of this party, which we believe would be not feasible, given the narrow time frame and anticipated unwillingness. Second, we wanted the emails to be equally relevant to all participants, because previous studies have showed that (perceived) relevance has impact on susceptibility rates. We believed it was less likely that a third-party sender would be equally relevant to all participants, compared to for example the email service of the Ministry of Economic Affairs. *Last*, the duration of the phishing mail experiment in total was six weeks, which implies only 6 weeks between the first and second phishing email, and 2 weeks between the last infographic -and second phishing email. Perhaps the limited time between interventions and measurement, was of influence on the effectiveness of interventions. This could have been enhanced due to the resemblance of both emails. However, due to time constraints, we could not deviate from this planning.

5.5 Future research

Since most of these limitations have been imposed due to technical or time constraints, we suggest these can be overcome by future research. Furthermore we propose some future directions based upon our findings. *First*, we suggest future research should expand the scope of our research focused on screen locking behaviour. By including multiple buildings, this could limit possible intervention spill over effects, as also it could contribute to a better grounded generalization of findings. However, building specific characteristics should be taken into account and need to be correct for, as much as possible. *Furthermore*, we also propose to extend the time frame of intervention period, as done in most salient reminders studies. We expect that by expanding the time scope of this experiment, differences in results of information provision and salient reminders may be enhanced. However, to our knowledge, this has yet to be studied. *Moreover*, we propose to test whether treatments had impact on participants using the suggested hotkey combination or on the general tendency of locking your screen. As many studies focuses on the direct link of reminders on behaviour (e.g. flashlights near alcohol dispensers, poster near elevators or stairs etc.), we like to see its implications tested, in the field of information secure behaviour.

Also as noted in the discussion of our phishing mail experiment, we suggest further research on the topic of what causes having previous experience with phishing emails to be effective. Although several studies have discussed the impact of previous experience, limited support is found on what causes it to be effective. For example, since meta-analysis conducted by Kluger & DeNisi (1996) found strong support for feedback interventions to improve behaviour, simulating previous experience with phishing mails with- and without feedback can be tested to gain more insights in what causes previous experience with phishing emails to reduce susceptibility to phishing fraud. *In addition*, the study can be repeated, to test the effect of the expansion of the time frame of treatment- and test moments, and to analyse treatment effects for third party senders, non-similar emails and harder/easier to recognize phishing emails. *Besides*, research could be expanded by a more in depth analyses of participants. This could clarify and give more meaning to our found effects, which determined participants those at highest risk (e.g. age, gender, employee contract, and organizational division). Last, we propose future research could be conducted on information treatments with the inclusion of phishing website and treatments without (such as in our experiment). This could support or undermine our proposed explanation of differences in results regarding the number participants who had visited the link and/or filled in passwords.

Chapter 6: Conclusion

In this study we aimed to analyse the human factor in information security. More specifically, how information secure behaviour can effectively be promoted in an organizational context. To do so, we conducted two field experiments regarding manually locking your screen and phishing. *The first step we took was to analyse "why" individuals perform information (in)secure behaviour.*

In Chapter two we proposed that computer end-users lack of knowledge, experience and attention to incoming mails, are the most relevant factors describing one's susceptibility to *phishing* fraud. Furthermore poor risk communication and proper guidelines, distributed responsibility and demographic factors also influence susceptibility. Moreover, non-compliance with the procedure of *locking your screen* is most influenced by; (1) low perceived risk, (2) effort and hindrance with daily work, (3) lack of knowledge, and (4) social influence.

After we had established the determinants of information (in)secure behaviour, we proposed interventions based upon behavioural insights to be the solution for "what" we can do to improve behaviour. Furthermore, before we started testing our interventions we discussed existing literature of "what" factors influence the effectiveness of treatments.

We stated that information provision can be effective to engage individuals in more protective and secure behaviour, although it is dependent on how- and which information is being communicated and processed. Information should include both the communication of threats (fear appeal), as well as an effective coping strategy (appropriate steps of prevention). Furthermore, effectiveness can be enhanced by incorporation of social norms and the rehearsal of policies and procedures (e.g. listing information companies would never ask) as well as by keeping messages short and simple and adding supportive cartoons/images. Furthermore it is important to present information in the form that is suitable for- and recognizable by the target group.

Moreover, the generation of experience with phishing as intervention strategy (by simulating an attack), is also referred to as promising. Due to learning-by-doing and provided feedback, this could generate know-how over- and familiarization with phishing, during the normal use of email. It is mentioned to be more effective than simple information provision, since it not only increases awareness (which could also help to avoid phishing fraud), but also makes users more knowledgeable about techniques they can use to identify phishing, accompanied with higher levels of attention.

Last, we proposed changing information insecure behaviour, by making use of constant salient reminders. Increasing the salience of a particular option or behaviour, will make it easier to process, and therefore makes that option more appealing. It can even be effective in changing behaviour, to the extent of generating habitual behaviour. In this case the behavioural change remains, although reminders have been stopped. One crucial element of the effectiveness of reminders is that it is largely dependent on when, where and how reminders are presented to individuals.

Interventions in order to be effective must achieve all or a selection of the following changes; (1) altered risk perceptions, (2) increased awareness, attention and knowledge (self-efficacy) to show that information secure behaviour is compatible with daily tasks, (3) better understanding of policies and procedures, and (4) sense of responsibility of the end-user. After we have diagnosed the 'hypothetically' effectiveness of our suggested interventions we continued our 'quest' by bridging the gap of "what" can be done to improve information secure behaviour and "how" effective these interventions contribute to information secure behaviour. In short, to see "which" interventions are more or less effective than others.

To ensure reduction of susceptibility, we tested the effectiveness of security education, training and awareness programs in the form of information provision and simulating previous experience with phishing emails. We found, compared to the control group, all treatments to reduce susceptibility to phishing fraud. Furthermore, generating previous experience with *phishing emails* was more effective in than providing information. However, findings were contrary to those of Bowen et al. (2010), Kumaraguru et al., (2007) and Sheng et al., (2007), since we did not find the combination of treatments to be more effective than one of both.

The reason for generating previous experience with phishing fraud to be more effective than simply informing over phishing, is supposed to come from familiarization with the phishing scam as a whole and that information could be simply neglected (contrary to the experience treatment). We expect that those who received a phishing mail in advance, have gain knowledge of both stages in which participants could have detected phishing. Furthermore, we believe that in line with findings Kluger & DeNisi (1996) feedback to be an important factor driving the effectiveness of simulating previous experience with phishing fraud. Although, participants only received a very brief debriefings statement, this enabled them to analyse its consequences and to adapt if necessary (Hermsen et al., 2016).

Furthermore, in our *screen locking experiment*, we found constant salient reminders and information to be effective in increasing the ratio of manual locks of total locks and number of times participants manually locked their screen. Compared to the control group, this holds for the intervention period, and the periods two weeks- and two months after treatments were stopped. In the intervention and period two weeks after treatments were stopped, the combined treatment was most effective in promoting information secure behaviour. We found long-lasting treatment effects, two months after treatments were stopped, for all three treatments. Therefore, in line with findings of Calzolari & Nardotto (2015), Taubinsky (2014) and Zurovac (2011) we found constant salient reminders to be effective in the long-run. Unanticipated, we found no differences in treatment effectiveness between the information provision treatment, compared to the two (constant) salient reminder treatments ((constant) salient reminder and combined treatment). However, in both treatments in which participants were given information (flyers) (information provision- and combined treatment), the number of times participants manually locked their screen declined over time. The question remains whether differences in treatment effectiveness between information provision and (constant) salient reminders will increase over time, or not.

*In this chapter we have finalized our 'quest' of human behaviour in information security. In order to answer the question, **how information secure behaviour can be effectively promoted in an organizational context**, we have discussed "why" individuals behave information (in)secure and "what" we hypothetically can do to improve such behaviour. This took us to the next level, in which we tested "which" and "how" effective proposed interventions are in enhancing information secure behaviour. Based on our main findings, we gave both practical as scientific implications and listed limitations and directions for future research.*

Appendices

Appendix 3.1. PM: Kruskal-Wallis test results group formation

Table A.3.1. PM: Kruskal-Wallis equality-of-populations rank test: Age

Group	Obs	Rank Sum
1	2723	1,50e+07
2	2740	1,51e+07
3	2724	1,47e+07
4	2742	1,50e+07

Chi-squared = 2,479

Probability = 0,4790

Chi-squared with ties = 2,481

Probability = 0,4787

Table A.3.2. PM: Kruskal-Wallis equality-of-populations rank test: Age_Group

Group	Obs	Rank sum
1	2723	1,50e+07
2	2740	1,51e+07
3	2724	1,47e+07
4	2742	1,50e+07

Chi-squared = 3,697

Probability = 0,2961

Chi-squared with ties = 9,980

Probability = 0,2636

Table A.3.3. PM: Kruskal-Wallis equality-of-populations rank test: Gender

Group	Obs	Rank sum
1	2723	1,49e+07
2	2740	1,50e+07
3	2724	1,48e+07
4	2742	1,50e+07

Chi-squared = 0,508

Probability = 0,9172

Chi-squared with ties = 0,708

Probability = 0,8712

Table A.3.4. PM: Kruskal-Wallis equality-of-populations rank test: Int_employee

Group	Obs	Rank sum
1	2723	1,49e+07
2	2740	1,48e+07
3	2724	1,50e+07
4	2742	1,50e+07

Chi-squared = 0,932

Probability = 0,8177

Chi-squared with ties = 0,1957

Probability = 0,5814

Table A.3.5. PM: Kruskal-Wallis equality-of-populations rank test: Organizational subdivision

Group	Obs	Rank sum
1	2723	1,48e+07
2	2740	1,53e+07
3	2724	1,53e+07
4	2742	1,44e+07

Chi-squared = 21,256

Probability = 0,0001

Chi-squared with ties = 23,142

Probability = 0,0001

Appendix 3.2. PM: Security notice prior to phishing mail field experiment

Hou je wachtwoord geheim!

Geef je wachtwoord om in te loggen op je werkplek nooit aan anderen, en weet dat je werkgever en andere instanties nooit zullen vragen je wachtwoord op te sturen.

Recent is via diverse media gewaarschuwd voor spam- en phishingmails die momenteel in omloop zijn (o.a. CJIB, ING en ICS). Op het werk kun je ook met spam- en phishingmails te maken krijgen. Volgens het [Reglement voor de Digitale werkplek \[link\]](#), moet je je wachtwoord elke 60 dagen veranderen. Uiteraard kun je je wachtwoord ook eerder wijzigen, als je vermoedt dat je wachtwoord niet langer geheim is.

Vragen?

Bij vragen kun je contact opnemen met de [Informatiebeveiligingscoördinator](#) van jouw organisatie.

Appendix 3.3. PM: Standard answers incoming mails and phone calls

Telefonie protocol / instructie DICTU Servicedesk projectteam Front Office

- **Situatie wanneer mensen de mail niet vertrouwen/ de mail willen melden als phishing:**

1. Klant belt naar de DICTU Servicedesk en geeft aan dat hij/zij een mail ontvangen heeft die niet gewenst is c.q. die hij/zij niet vertrouwt (vermoeden van phishing).
2. De DICTU Servicedesk stelt twee controle vragen om te constateren, of het de bewuste mail gaat:
 - i. Wie is de afzender ?
 - ii. Wat is het onderwerp?

3. De DICTU Servicedesk vraagt de medewerker om de mail, conform Antispam/Phishing richtlijnen, als bijlage door te sturen naar de DICTU Servicedesk.

De instructie hiervoor is:

Open in Microsoft Outlook een nieuw bericht;

Selecteer het menu "INVOEGEN"

en vervolgens "OUTLOOK-ITEM";

Selecteer nu het betreffende e-mail bericht in "POSTVAK IN" en voeg dit toe als bijlage aan de nieuwe e-mail;

Stuur de nieuwe e-mail met bijlage naar de postbus servicedesk@dictu.nl;

- **Situatie wanneer mensen de mail niet als verdacht zien maar vragen hebben over de inhoud van de mail**

Standaard antwoord is:

Bedankt voor deze melding met je vragen. Wij hebben meer vragen ontvangen over dit onderwerp. De behandeling en beantwoording daarvan vergt enige tijd. Wij verwachten dat je hierover binnen 3 werkdagen een inhoudelijke reactie ontvangt.

Ten alle tijde: belangrijk dat er NIET gemeld wordt:

- dat het om een actie of onderzoek gaat
- dat het niet echt is

Om zo medewerkers niet te beïnvloeden.

FAQ's van medewerkers verdeeld in een aantal categorieën:

De medewerker met een **inhoudelijke** vraag:

Mobile Password Recovery System

Hoe kan het dat ik nergens informatie kan terugvinden over het verhogen van mijn Outlook exchange Limiet

Ik kan niks vinden op intranet over het verhogen van mijn Outlook exchange Limiet?

Ik heb mijn mailbox niet verhoogd. Kan ik nog steeds gebruik maken van mijn outlook?

Ik heb mijn mailbox niet verhoogd, maar ik kan nog steeds gebruik maken van mijn mail. Hoe kan dit?

Kan DICTU zelf niet gewoon regelen dat de mailbox wordt verhoogd. Waarom zou ik daarvoor gegevens moeten invullen.

Ik ben naar de Servicebalie gegaan, maar die weten van niks?

Geldt dit voor alle organisatieonderdelen?

Ik weet mijn gebruikersnaam/wachtwoord/telefoonnummer niet?

Mijn leidinggevende weet niks van dit onderwerp af. Hoe kan dit?

Standaard telefonische antwoord voor medewerkers met inhoudelijke vragen

Bedankt voor deze melding met je vragen. Wij hebben meer vragen ontvangen over dit onderwerp. De behandeling en beantwoording daarvan vergt enige tijd. Wij verwachten dat je hierover binnen 3 werkdagen een inhoudelijke reactie van ontvangt.

De medewerker die denkt/weet (**vermoeden**) dat hij/zij een phishingmail heeft ontvangen

Ik denk dat ik een phishingmail heb ontvangen, wat moet ik doen? :

Als het daadwerkelijk de nep phishingmail betreft is het antwoord:

Bedankt voor het melden van dit verdachte mailtje. Er zijn al meer meldingen geweest hierover. Er is geen dreiging ontstaan en je (persoonlijke) accountgegevens zijn niet in gevaar geweest (ook niet als je eventuele gegevens hebt ingevuld). We adviseren je om de phishingmail te verwijderen. Daarna hoef je verder **geen** vervolgacties te ondernemen.

Ik heb op de link in de mail geklikt, loop ik nu gevaar? :

Antwoord: Nee, want we hebben de dreiging kunnen neutraliseren. Er waren al meer meldingen geweest. Bedankt voor de melding; u kan de mail verwijderen.

Ik heb gegevens ingevuld op de website, moet ik nu mijn wachtwoord veranderen?

Antwoord Nee, want we hebben de dreiging kunnen neutraliseren. Er waren al meer meldingen geweest. Bedankt voor de melding; u kan de mail verwijderen.

Moet ik mijn leidinggevende inschakelen?

Antwoord Nee, want we hebben de dreiging kunnen neutraliseren. Er waren al meer meldingen geweest. Bedankt voor de melding; u kan de mail verwijderen

Als het een andere phishingmail betreft: vraagt de medewerker om de mail, conform Antispam richtlijnen (dus als bijlage), als bijlage door te sturen naar de DICTU Servicedesk.

Mail protocol / instructie DICTU Servicedesk projectteam Front Office

Algemeen

Mail komt binnen in de map "Mailing actie DB" onder FO (Front Office).

Hier staan de te behandelen e-mails. Als je een mail in behandeling neemt zet je je initialen in het onderwerp veld van de e-mail.

Na behandeling verplaats je de e-mail naar de map "Afgehandeld" onder de map "Mailing actie DB".

Sjabloon I betreft klanten die vermoeden dat het phishing is en de mail doorsturen naar de Servicedesk. Hierbij is het duidelijk dat het om de nep phishing e-mail gaat.

Sjabloon II betreft klanten die vermoeden dat het phishing is en waarbij het nog niet met zekerheid te zeggen is, om welke phishing e-mail het gaat. Hierbij vraag je d.m.v. sjabloon II aan de klant om de phishing e-mail als bijlage naar de Servicedesk te sturen. Na ontvangst door de Servicedesk van de phishing mail (als bijlage) wordt alsnog sjabloon I naar de klant gestuurd.

Sjabloon III betreft klanten die het niet als een verdachte e-mail zien, maar vragen stellen over de inhoud. Ze gaan er dus echt op in.

Mail ALTIJD versturen uit de postbus DICTU Servicedesk!

Sjabloon I "phishingmail is mee/doorgestuurd"

Beste collega,

Bedankt voor het melden van deze verdachte e-mail.

De DICTU Servicedesk heeft je melding in goede orde ontvangen.

Inmiddels hebben wij meerdere meldingen gehad. Er is geen sprake van een risico.

Je (persoonlijke) accountgegevens zijn niet in gevaar geweest (ook niet als je eventuele gegevens hebt ingevuld).

We adviseren je om deze e-mail te verwijderen. Deze zogenaamde phishing mails zijn een vorm van oplichting.

Mocht je over deze e-mail een inhoudelijke vraag hebben gesteld:

Je kunt hierover binnen 3 werkdagen een reactie verwachten.

Je hoeft voor deze e-mail verder zelf **geen** vervolgacties te ondernemen.

Met vriendelijke groet,

DICTU Servicedesk.

Sjabloon II "phishing mail alsnog even toesturen"

Beste collega,

Bedankt voor het melden van deze verdachte e-mail. Om je melding verder in behandeling te nemen verzoeken wij je om de ontvangen e-mail als bijlage toe te sturen naar de DICTU Servicedesk. Hierdoor kunnen dit soort e-mails worden opgenomen in het spam filter.

Open in Microsoft Outlook een nieuw bericht;
Selecteer het menu "INVOEGEN"
en vervolgens "OUTLOOK-ITEM";
Selecteer nu het betreffende e-mail bericht in "POSTVAK IN" en voeg dit toe als bijlage aan de nieuwe e-mail;
Stuur de nieuwe e-mail met bijlage naar de postbus servicedesk@dictu.nl;

We adviseren je om de oorspronkelijke e-mail te verwijderen.
Deze zogenaamde phishing mails zijn een vorm van oplichting.

Je hoeft verder zelf **geen** vervolgacties te ondernemen.

Met vriendelijke groet,

DICTU Servicedesk.

Sjabloon III inhoudelijke mailvragen

Wanneer gebruiken: De klant ziet het niet als een phishing e-mail en heeft vragen gesteld over de inhoud van het Mobile Password Recovery System. Dus alle mogelijke vragen die geen betrekking hebben over een phishing e-mail.

Antwoord:

Beste collega,

Bedankt voor deze melding met je vragen. Wij hebben meer vragen ontvangen over dit onderwerp. De behandeling en beantwoording daarvan vergt enige tijd. Wij verwachten dat je hierover binnen 3 werkdagen een reactie van de Directie Bedrijfsvoering ontvangt.

Met vriendelijke groet,

DICTU Servicedesk.

Appendix 3.4. PM: Phishing mail 1 (simulated experience treatment)

AFZENDER : Directiebedrijfsvoering@Minez.nl

Onderwerp: ACTIVEER nu uw Mobile Password Recovery System



Beste EZ -Medewerker

Na een succesvolle pilot van de Directie Bedrijfsvoering, zijn wij onlangs gestart met het implementeren van het EZ - Mobile Password Recovery System (EZ-MPRS) voor alle EZ-medewerkers. Hiermee kunt u, ten alle tijden, uw wachtwoord van uw gebruikersaccount, opvragen en wijzigen. Hiermee hopen we u nog sneller en beter van dienst te kunnen zijn.

Uit onze gegevens blijkt dat u nog geen gebruik maakt van het EZ - Mobile Password Recovery System. Daarom vragen we u , éénmalig, uw gebruikersaccount te koppelen aan uw mobiele nummer.

Activeer [hier](#) uw EZ – Mobile Password Recovery System (MPRS)

Voor meer informatie, zie onderstaande link:

<https://rijksweb.nl/ezmprs>

Met vriendelijke groet,

Directie Bedrijfsvoering

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is gezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

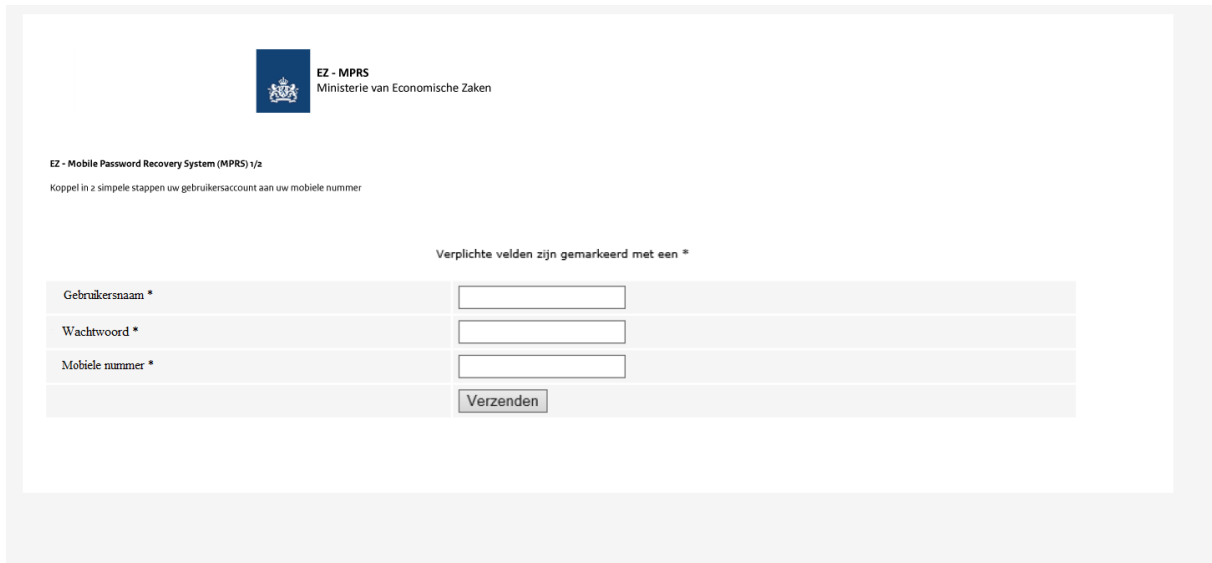
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages




Appendix 3.5. PM: Website first phishing mail and pop-up screen

Website first phishing mail : first screen

- www.mobilepasswordrecoveryssystem.net



 **EZ - MPRS**
Ministerie van Economische Zaken

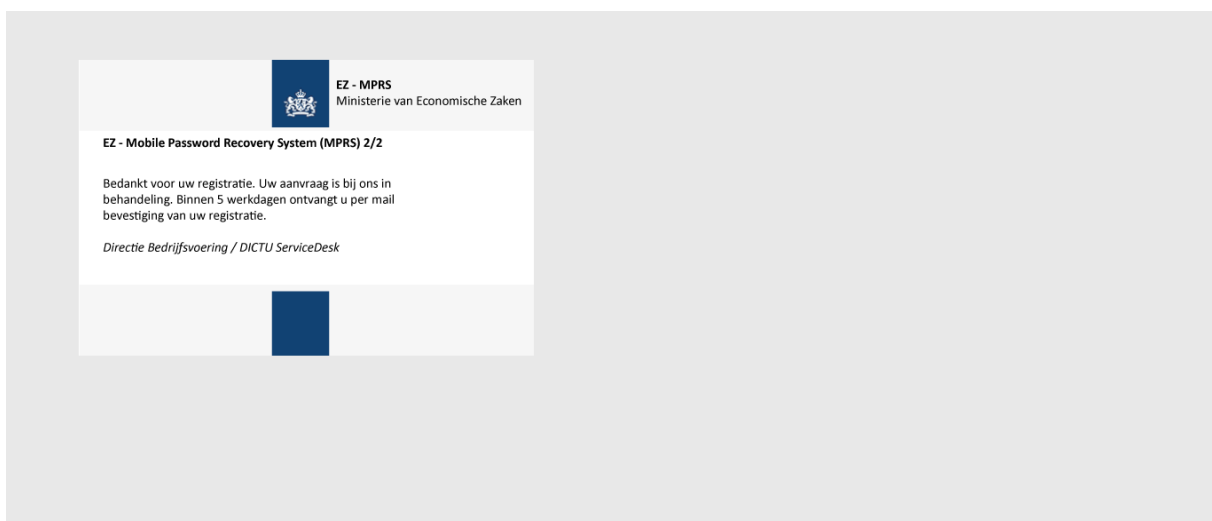
EZ - Mobile Password Recovery System (MPRS) 1/2
Koppel in 2 simpele stappen uw gebruikersaccount aan uw mobiele nummer


Verplichte velden zijn gemarkeerd met een *

Gebruikersnaam *	<input type="text"/>
Wachtwoord *	<input type="password"/>
Mobiele nummer *	<input type="text"/>
<input type="button" value="Verzenden"/>	

Website first phishing mail : second screen (redirected screen)

- www.mobilepasswordrecoveryssystem.net/gekoppeld.php




 **EZ - MPRS**
Ministerie van Economische Zaken

EZ - Mobile Password Recovery System (MPRS) 2/2


Bedankt voor uw registratie. Uw aanvraag is bij ons in behandeling. Binnen 5 werkdagen ontvangt u per mail bevestiging van uw registratie.

Directie Bedrijfsvoering / DICTU ServiceDesk


Appendix 3.6. PM: Short debriefing after first phishing mail




Ministerie van Economische Zaken



'Imitatie' Phishing mail




Je hebt vandaag een 'imitatie' phishingmail ontvangen, met afzender Directie Bedrijfsvoering. Deze mail, met het onderwerp EZ Mobile Password Recovery System, was een 'imitatie' phishingmail, ontworpen met het doel om je bewustzijn op het gebied van phishing te vergroten. Op deze manier kunnen we samen bijdragen aan een veiligere digitale werkomgeving. Kwaadwillenden kunnen via phishingmails, misbruik maken van je gegevens.



LET OP!

Als je je wachtwoord hebt ingevuld, wijzig dit dan nu meteen! Dit kan door gebruik te maken van de toetsencombinatie; **Control + ALT + DEL**, en dan te kiezen voor: "Wachtwoord wijzigen". Ondanks genomen veiligheidsmaatregelen, zijn veiligheidsrisico's nooit volledig uit te sluiten. Mocht je de phishingmail naar iemand hebben doorgestuurd, dan vragen wij je deze persoon hierover ook in te lichten (m.u.v. [DICTU Servicedesk](mailto:DICTU_Servicedesk) en antispam@dictu.nl).



We danken je hartelijk voor je bijdrage aan een veiligere digitale werkomgeving. Om de situatie van een phishingmail zo realistisch mogelijk te benaderen, is gekozen om je niet van tevoren in te lichten. We vragen hiervoor je begrip. Voor vragen omtrent deze 'imitatie' phishingmail, kan je terecht bij de IB-coördinator van jouw organisatiedeel.

Appendix 3.7. PM: Infographics (Information provision treatment)

Ministerie van Economische Zaken

Beste collega,

Vorig jaar oktober organiseerde de directie Bedrijfsvoering de aftrap van de campagne iBewustzijn bij EZ; een groot succes!

Het doel van deze rijksbrede campagne is je digitale vaardigheden trainen en verbeteren én veiligheidsrisico's herkennen en voorkomen. Daarom ontvang je deze maand drie informatieve mails over het onderwerp 'phishing'. Wil je deze mails aandachtig lezen? Op die manier vergroot je je eigen digivaardigheden op het gebied van: (1) Wat is phishing?, (2) Hoe herken je een phishingmail?, en (3) Wat moet je doen als je denkt/weet een phishingmail te hebben ontvangen?

Meer informatie over iBewustzijn vind je onder meer op <https://www.ibewustzijnoverheid.nl>

Vriendelijke groet,

Johan Maas
Directeur Bedrijfsvoering

Digivaardigheden – phishingmails (1)

1

2

3

Wat is phishing?

Hoe herken ik phishing?

Een phishingmail, en nu?

Wat is phishing?

De 'phisher'

Phishing is een vorm van internetfraude. Bij phishing proberen fraudeurs (phishers) via e-mail je persoonlijke inlog- en/of bankgegevens te achterhalen.

De 'phisher' heeft nu controle over je account.

Je komt vervolgens op een nepsite. Daar wordt gevraagd om je account te controleren en te verifiëren door in te loggen.

Kenmerkend voor een phishingmail is de dreigende toon. Bijvoorbeeld dat als je niet inlogt, je geen gebruik meer kunt maken van je account of bankrekening of dat je een veiligheidsrisico loopt. Om in te loggen, moet je eerst op een link in de e-mail klikken.

Phishing via Social Media

De 'phisher'

De 'phisher' zoekt op internet en social media naar bruikbare informatie (waar je werkt etc.) om zijn doelwit op persoonlijke wijze uit naam van die organisatie, te benaderen.

Met de online gevonden informatie, benadert de 'phisher' zijn doelwit, zogenaamd uit naam van de organisatie.



Ministerie van Economische Zaken



Digivaardigheden – phishingmails (3)



Hoe reageer ik op een (mogelijke) phishingmail?



- Klik NIET op de link.
- Geef nooit inloggegevens of vertrouwelijke informatie.
- Stuur de mail als bijlage naar **antispam@dictu.nl**.
- **RVO:** Ook CC aan rvoinformatiebeveiliging@rvo.nl
- **NVWA:** Ook CC aan beveiligingsincidentmelding@nvwa.nl



Vragen over verdachte mails? - Contactgegevens:

- **DICTU Servicedesk**

Telefoonnummer: 070 378 6666 (66666) **voor:** KD & SODM
088 602 8888 (8888) **voor:** RVO & NVWA
AT & DICTU

Emailadres: servicedesk@dictu.nl

- **De IB - Coördinator(en) van je organisatieonderdeel**
- **Rijksportal (Informatiebeveiliging)**
 - Intranet van je organisatieonderdeel

Meer weten?

- <https://www.ibewustzijnoverheid.nl>
- <https://veiliginternetten.nl>



Ministerie van Economische Zaken



Digivaardigheden – phishingmails (3)



Hoe reageer ik op een (mogelijke) phishingmail?



- Klik **NIET** op de link.
- Geef nooit inloggegevens of vertrouwelijke informatie.
- Stuur de mail als bijlage naar **antispam@dictu.nl**.
- **RVO:** Ook CC aan: rvoinformatiebeveiliging@rvo.nl
- **NVWA:** Ook CC aan beveiligingsincidentmelding@nvwa.nl



Vragen over verdachte mails? - Contactgegevens:

• DICTU Servicedesk

Telefoonnummer: 070 378 6666 (66666) **voor:** KD & SODM
088 602 8888 (8888) **voor:** RVO & NVWA
AT & DICTU

Emailadres: servicedesk@dictu.nl

- De **IB - Coördinator(en) van je organisatieonderdeel**
- **Rijkspportaal (Informatiebeveiliging)**
 - Intranet van je organisatieonderdeel

Meer weten ?

- <https://www.ibewustzijnoverheid.nl>
- <https://veiliginternetten.nl>

Appendix 3.8. PM: Phishing mail 2

AFZENDER : helpdesk@dlctu.nl

Onderwerp: VERHOOG je Outlook Exchange email opslaglimiet



Beste EZ-medewerker,

Uw mailbox heeft de toegestane opslaglimiet overschreden die is ingesteld door DICTU. U mag geen e-mail meer verzenden of ontvangen totdat u de upgrade van het toegewezen quotum hebt uitgevoerd. Voor het verhogen van uw quotum klikt u op onderstaande link:

Verhoog [hier](#) uw opslaglimiet

Als u dit niet doet loopt u het risico dat uw mailaccount wordt afgesloten. Hartelijk dank voor uw medewerking.

Met vriendelijke groet,

Voor meer informatie, zie onderstaande link:

<https://rijksweb.nl/exchangelimiet>

De DICTU Helpdesk

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is gezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

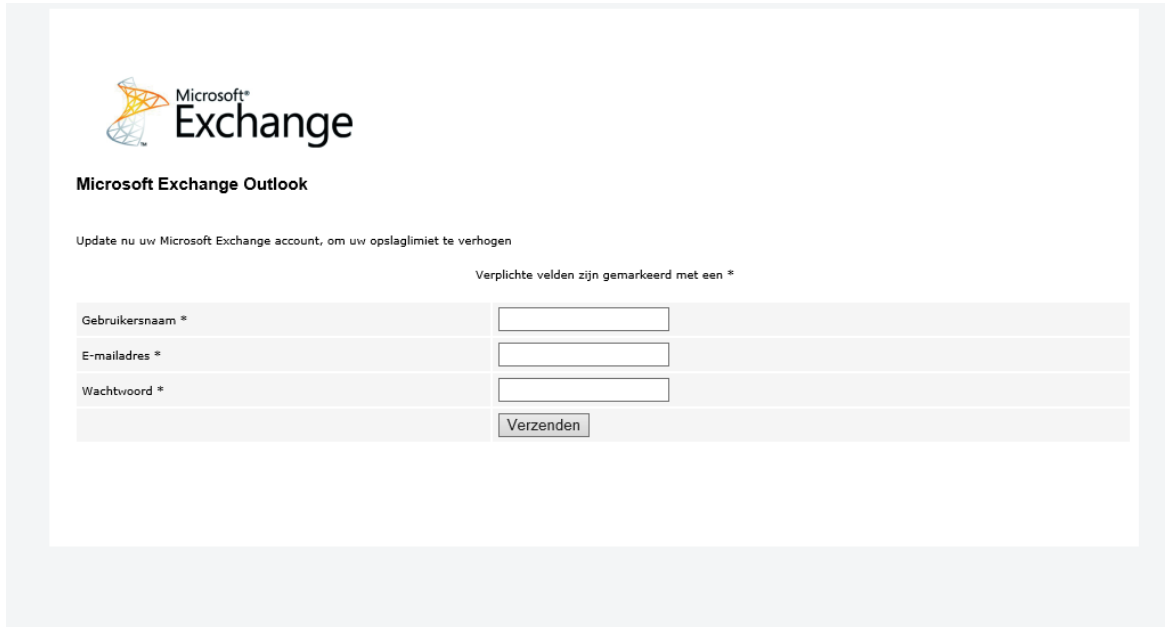
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.



Appendix 3.9. PM: Website second phishing mail and Pop-up screen

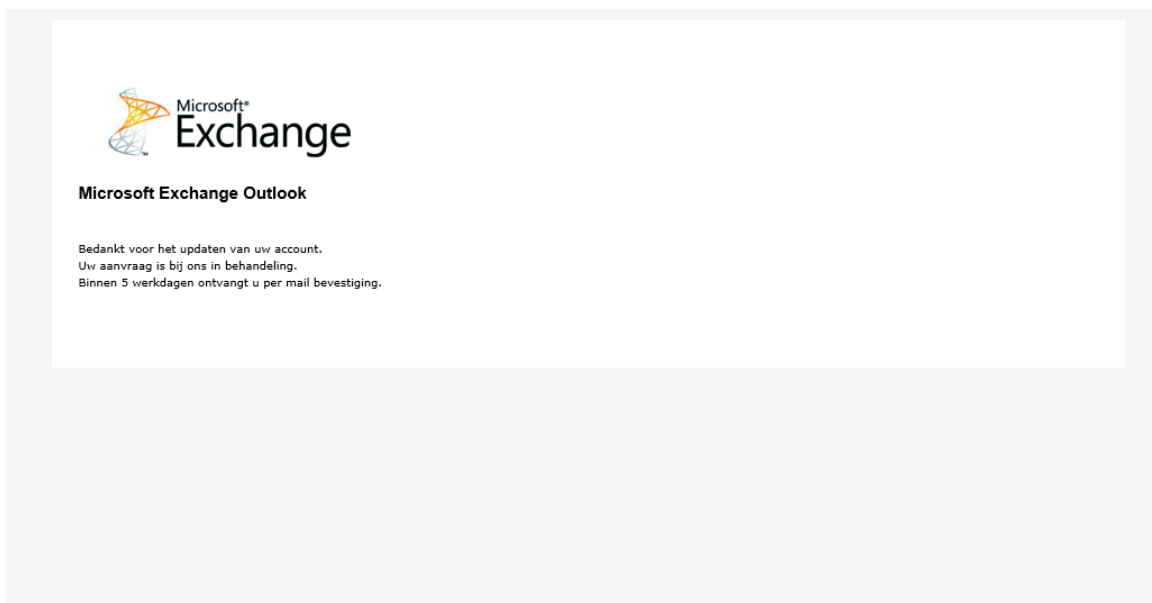
Website second phishing mail : first screen

- www.verhoogjeopslaglimiet.net



Website second Exchange phishing mail : second screen (redirected screen)

- www.verhoogjeopslaglimiet.net/verhoogd.php



Appendix 3.10. PM: General debriefing and explanation of the phishing field experiment



Woensdag 16 december 2015

Beste collega,

Gisteren heb je een e-mail ontvangen met als onderwerp: "Verhoog je Outlook Exchange email limiet" en met als afzender helpdesk@dlctu.nl. In deze mail werd je gevraagd op een link te klikken om je accountgegevens en wachtwoord in te vullen. Dit was een 'imitatie' phishingmail, een e-mail die kenmerken bevat van een phishingmail, met het doel om je bewustzijn op het gebied van phishing te verhogen.

Mocht je geklikt hebben op de link en/of gegevens ingevuld hebben, hoef je je geen zorgen te maken, deze mail heeft geen enkele consequentie. Het kan zijn dat je al eerder bericht over een eerdere imitatie phishingmail en informatie over phishing hebt ontvangen

Een kenmerk waaraan je een phishingmail kan herkennen is bijvoorbeeld een vreemde afzender. Bij de 'imitatie' phishingmail was dat helpdesk@dlctu.nl (let op het gebruik van *helpdesk* in plaats van *servicedesk* en de spelfout in *dlctu*). Daarnaast liet de link zien dat je geleid werd naar een website met een ongebruikelijke domeinnaam (verhoogjeopslaglimiet.**net**).

Deze mail is dus **niet** verzonden door de DICTU Servicedesk, maar DICTU heeft wel zijn medewerking verleend om deze actie mogelijk te maken. Om het leereffect in het herkennen van een phishingmail voor elke individuele medewerker zo groot mogelijk te houden, is aan DICTU gevraagd niet te communiceren naar medewerker over deze actie en geen berichten op Rijksportaal (intranet) te plaatsen.

Deze 'imitatie' phishingmail is verzonden in het kader van de campagne iBewustzijn door de Directie Bedrijfsvoering en het Behavioural Insights Team van Economische Zaken, na afstemming met de DOR en goedkeuring van de SG en HDIOU. Met deze mail willen wij je informeren over onderstaande punten:

1. De aanleiding
2. Het doel van deze actie
3. De aanpak
4. Omgang met (persoonlijke) gegevens
5. Contactpunt voor vragen en verdere informatie

1. Aanleiding

Phishing is een vorm van internetfraude waarbij fraudeurs (phishers) via e-mail persoonlijke inloggegevens proberen te achterhalen. Dit is een reële dreiging voor individuen en voor organisaties, ook voor EZ. Het is voor EZ belangrijk om zich hier tegen te wapenen, niet alleen op technisch vlak, maar ook door medewerkers te trainen in het herkennen van deze mails. Phishers sturen steeds realistischere mails, specifiek gericht op bedrijven en uit naam van bedrijven of organisaties om inloggegevens van medewerkers te achterhalen en zo systemen binnen te komen.

2. Het doel

Het doel van deze actie was driedig: (1) verhogen van het bewustzijn op het gebied van phishing, (2) in kaart brengen hoe kwetsbaar onze organisatie is voor phishingmails, én (3) testen wat de meest effectieve maatregelen zijn om de schadelijke effecten van phishingmails te beperken. Op deze manier kunnen we samen bijdragen aan een veiligere digitale werkomgeving.

3. De aanpak

Medewerkers van EZ zijn voor deze actie onderverdeeld in 4 verschillende groepen. In deze 4 groepen zijn verschillende maatregelen uitgetest, om de effectiviteit van verschillende maatregelen te onderzoeken. Onderzocht is wat de effecten zijn van het verschaffen van informatie en/of het hebben van een eerdere ervaring met phishingmails. Een uitgebreide beschrijving van de aanpak lees je in het bijgevoegde pdf bestand. De verwachting is dat de resultaten van deze actie in Februari (2016) bekend zijn.

4. Omgang met (persoonlijke) gegevens

Om de privacy van jou als medewerker te waarborgen, zijn er verscheidende maatregelen genomen. Eén daarvan is dat, heel bewust, in de analyses alleen wordt gekeken naar het gedrag op groepsniveau en niet naar gedragingen van personen.

Een uitgebreide beschrijving van de aanpak en hoe is omgegaan met (persoonlijke) gegevens lees je in het bijgevoegde pdf bestand.

Het is goed mogelijk dat je in je dagelijkse werkzaamheden, ondanks technische maatregelen die genomen worden, te maken krijgt met een phishingmail. Om de situatie van een phishingmail zo realistisch mogelijk te benaderen is gekozen om je niet van te voren in te lichten over deze actie. Wij vragen hiervoor je begrip.

5. Contactpunt voor vragen en verdere informatie

Een uitgebreide omschrijving van deze actie vind je in de bijlage van deze mail. Voor verdere vragen over deze actie en overige vragen omtrent informatieveiligheid kan je terecht bij de [IB-coördinator](#) van jouw organisatiedeel.

Vriendelijke groet,

Johan Maas
Directeur Bedrijfsvoering

Inleiding:

Internetgebruik is volledig geïntegreerd in ons dagelijks leven, zowel op werk- als op persoonlijk gebied. Echter, we zijn ons soms niet volledig bewust van de mogelijke gevaren. Om deze gevaren zo adequaat mogelijk te bestrijden, worden verschillende technische maatregelen genomen. Toch kunnen deze maatregelen nooit 100% waterdicht zijn, waardoor een beroep wordt gedaan op de laatst mogelijke verdedigingslinie, de menselijke factor.

Met deze actie is geprobeerd het bewustzijn van medewerkers op het gebied van phishing te verhogen. Tegelijkertijd is geprobeerd in kaart te brengen, wat de meest effectieve maatregelen zijn om de menselijke verdedigingslinie te versterken, namelijk in hoeverre informatie over en ervaring met phishingmails bijdragen aan een juiste herkenning van phishingmails.

Aanpak:

Alle EZ-medewerkers zijn onderverdeeld in vier groepen, waarin verschillende maatregelen zijn uitgetest. Enkele functies en organisatieonderdelen die niet onder de ICT servicedienstverlening van DICTU staan (ACM en CPB) zijn uitgesloten.

Sommigen van jullie hebben drie verschillende informatiemails ontvangen met de titels; (1) Informatiebeveiliging (IB): Wat is phishing ? (2) Informatiebeveiliging (IB): Hoe herken ik phishing?, en (3) Informatiebeveiliging (IB): Een phishingmail, en nu?. Sommigen van jullie hebben voorafgaand aan de imitatie phishingmail van DICTU een eerdere imitatie phishingmail ontvangen over een mobile password recovery systeem (afzender DB). De twee groepen die in een eerder stadium al een phishingmail hebben ontvangen hebben hierover al eerder bericht gehad. De onderzoeksopzet is hieronder schematisch weergegeven:

Groep/Tijd	Datum 5/11	Datum 19/11	Datum 26/11	Datum 3/12	Datum 15/12
Groep 1 - Controle	-	-	-	-	Phishingmail
Groep 2 - Informatie	-	Infomail 1	Infomail 2	Infomail 3	Phishingmail
Groep 3 - Phishingmail	Phishingmail	-	-	-	Phishingmail
Groep 4 - Informatie - Phishingmail	Phishingmail	Infomail 1	Infomail 2	Infomail 3	Phishingmail

De verwachting is dat de resultaten van deze actie in Februari (2016) bekend zijn.

Omgang met (persoonlijke) gegevens:

Uiteraard hebben we gedurende het onderzoek veel zorg en aandacht besteed aan jou als medewerker en jouw (persoonlijke) gegevens.

- Het onderzoek is afgestemd met informatiemanagers, IB-coördinatoren en de DICTU ServiceDesk medewerkers, zodat jij als werknemer ten alle tijden goed geholpen kon worden.
- Eventueel ingevulde gegevens zijn niet opgeslagen. Er is alleen opgeslagen óf er iets is ingevuld.
- Om mogelijke risico's en de privacy impact in kaart te brengen is een (wettelijk vastgestelde) Privacy Impact Analyse (PIA) opgesteld. Op basis van de PIA zijn maatregelen genomen om de privacy optimaal te borgen.
- De analyses en resultaten van dit onderzoek berusten uitsluitend op geanonimiseerde en geaggregeerde informatie.

Behavioural insights team (BIT) EZ:

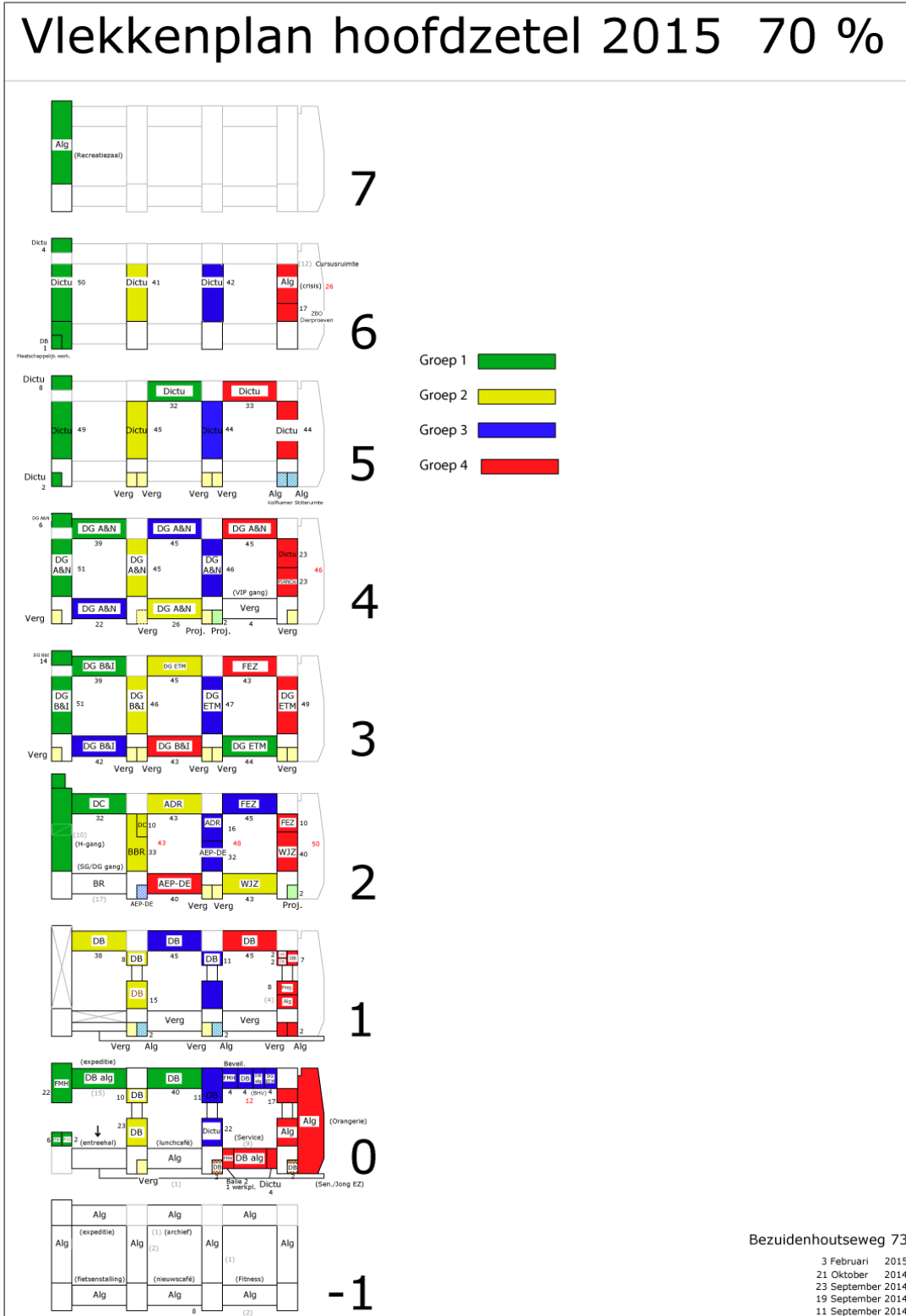
Deze actie is een samenwerking van Directie Bedrijfsvoering en het Behavioral Insights Team EZ (BIT). Het BIT ondersteunt beleidsdirecties en andere onderdelen van EZ bij het toepassen van gedragskennis in beleid. Het doel van het BIT is om door middel van inzicht in gedrag en het uittesten van beleidsinterventies, de effectiviteit van beleid verder te verhogen.

Wil je meer weten over de mogelijkheden van het BIT? Neem [hier](#) een kijkje.

Verdere vragen en informatie:

Voor overige vragen over deze actie of informatieveiligheid in het algemeen kun je terecht bij de [IB-coördinator](#) van jouw organisatiedeel.


Appendix 3.11. SL: Group formation Bezuidenhoutseweg 73



Appendix 3.12. SL: A5-Flyer (Information provision treatment)



Wist je dat:

- Je veelal werkt met vertrouwelijke informatie en bestanden
- 84 % van de EZ-medewerkers weet dat je altijd je computerscherm moet vergrendelen als je je werkplek verlaat
- Je heel gemakkelijk je computerscherm kunt vergrendelen door op de toetscombinatie  + L te drukken
- Je voor meer informatie terecht kunt op:
 - o <https://www.ibewustzijnoverheid.nl/>
 - o <https://veiliginternetten.nl/>

Dus daarom voordat je, je werkplek verlaat:



Appendix 3.13. SL: Stickers (constant salient remainder treatment)



16



17



¹⁶ Dimensions: 110 mm high by 15 mm wide

¹⁷ Dimensions: 14 mm high by 14 mm wide (round)

Appendix 4.1. *PM*: Comparing results of phishing mail experiment, with and without the exclusion of the NVWA

Table A.4.1. *PM*: Number of participants falling for phishing fraud per condition (in exact numbers and percentages).

Group	N	Visit the site	Username	E-mail	Password
<i>Control</i>	1803 (2723)	584-32,4% (877-32,2%)	402-22,1% (598-22,0%)	401-22,2% (597-21,9%)	399-22,1% (593-21,8%)
<i>Information provision</i>	2203 (2740)	530-24,1% (701-25,6%)	321-14,6% (448-16,4%)	321-14,6% (448-16,4%)	320-14,5% (446-16,3%)
<i>Simulated experience</i>	1986 (2724)	384-19,3% (635-23,3%)	214-10,8% (373-13,7%)	214-10,8% (373-13,7%)	212-10,7% (370-13,6%)
<i>Combined treatment</i>	2002 (2742)	449-22,4% (656-23,9%)	246-12,3% (356-13,0%)	246-12,3% (356-13,0%)	242-12,1% (351-12,8%)
<i>Total</i>	7976 (10929)	1947 - 24,4% (2869-26,3%)	1183-14,8% (1775-16,2%)	1182-14,8% (1774-16,2%)	1173-14,7% (1760-16,1%)

*(absolute numbers and percentage of participant **with** the **NVWA** included)

Table A.4.2. *PM*: Percentage of participants who clicked on the embedded link in the phishing mail, disaggregated per treatment group and organizational unit (with the NVWA included).

Group	Organizational unit					Total
	<i>AT</i>	<i>RVO</i>	<i>NVWA</i>	<i>KD</i>	<i>DICTU</i>	
Control		29,9% (891)*	31,9% (920)	36,9% (526)	32,1% (368)	32,2% (2723)
Information provision	34% (262)	20,9% (1233)	31,8% (537)	23,3% (373)	28,7% (335)	25,6% (2740)
Simulated experience		18,6% (1019)	34% (738)	22,2% (690)	15,2% (277)	23,3% (2724)
Combined treatment		21,8% (891)	28,0% (740)	22,5% (769)	24,0% (342)	23,9% (2742)
<i>Total</i>	34% (262)	22,8% (4034)	31,4% (2935)	26,2% (2358)	25% (1322)	26,3% (10929)

*(total number of participants per treatment group and organizational unit in brackets)

Table A.4.3. *PM*: Percentage of participants who filled in in password disaggregated, per treatment group and organizational unit (with the NVWA included).

Group	Organizational unit					Total
	<i>AT</i>	<i>RVO</i>	<i>NVWA</i>	<i>KD</i>	<i>DICTU</i>	
Control		21% (891)	21,1% (920)	25,5% (526)	21,2% (368)	21,8% (2723)
Information provision	24,8% (262)	13% (1233)	23,5% (537)	11,8% (373)	15,2% (335)	16,3% (2740)
Simulated experience		9,9% (1019)	21,4 % (738)	13,5% (690)	6,5% (277)	13,6% (2724)
Combined treatment		12,0% (891)	14,7% (740)	12,6% (769)	11,1% (342)	12,8% (2742)
<i>Total</i>	24,8% (262)	14,0% (4034)	20,2% (2935)	15,9% (2358)	13,5% (1322)	16,1% (10929)

*(total number of participants per treatment group and organizational unit in brackets)

Table A.4.4. PM: Overview χ^2 test results - Participants clicking on the embedded link per treatment

	Information	Experience	Combined
Control	$\chi^2=29,165$; P= 0,000***	$\chi^2=53,739$; P= 0,000***	$\chi^2=46,443$; P= 0,000***
Information		$\chi^2=3,819$; P= 0,051* ¹⁸	$\chi^2=2,027$; P= 0,155
Experience			$\chi^2=0,285$; P= 0,594 ¹⁹

* P<0,10 **P<0,05 *** P<0,01

(With the NVWA included)

Table A.4.5. PM: Overview χ^2 test results - Participants filled in their password per treatment

	Information	Experience	Combined
Control	$\chi^2=26,825$; P= 0,000***	$\chi^2=62,830$; P= 0,000***	$\chi^2=77,041$; P= 0,000***
Information		$\chi^2= 7,806$; P= 0,005***	$\chi^2=13,331$; P= 0,000*** ²⁰
Experience			$\chi^2=0,730$; P= 0,393

* P<0,10 **P<0,05 *** P<0,01

(With the NVWA included)

Table A.4.6. PM: Overview χ^2 test results- Participants who filled in their password of those who clicked on the link embedded in the phishing mail.

	Information	Experience	Combined
Control	$\chi^2=2,76$; P=0,096** ²¹	$\chi^2=13,92$; P=0,000***	$\chi^2=31,58$; P=0,000***
Information		$\chi^2=4,02$; P=0,045** ²²	$\chi^2=14,31$; P=0,000*** ²³
Experience			$\chi^2= 2,97$; P=0,085* ²⁴

* P<0,10 **P<0,05 *** P<0,01

(With the NVWA included)

¹⁸ With NVWA included significant (P<0,10); without significant (P<0,01)¹⁹ With NVWA included insignificant (P>0,10); without significant (P<0,05)²⁰ With NVWA included significant (P<0,01); without significant (P<0,05)²¹ With NVWA included significant (P<0,10); without significant (P<0,01)²² With NVWA included significant (P<0,05); without insignificant (P>0,10)²³ With NVWA included significant (P<0,01); without significant (P<0,05)²⁴ With NVWA included significant (P<0,10); without insignificant (P>0,10)

Table A.4.7. PM: Logistic regression results, with participants clicked the embedded link in the phishing mail as independent variable (with the NVWA included)

M2_VisitlinkBIN LOGIT	Coef.	Std. Err.	z	P>z	95% Confidence Interval	
1.male	0,2269296	0,0485095	4,69	0,000	0,1318528	0,3220064
1.Int_Employee	0,1337988	0,0676920	1,98	0,048	0,0011248	0,2664724
Group						
Information treatment	-0,3125279	0,0633745	-4,93	0,000	-0,4367396	-0,1883161
Experience treatment	-0,4191509	0,0619921	-6,76	0,000	-0,5406532	-0,2976485
Combined treatment	-0,4026685	0,0615052	-6,55	0,000	-0,5232165	-0,2821205
d_organisatieonderdeel						
DICTU	-0,3436189	0,1561138	-2,20	0,028	-0,6495964	-0,0376413
KD	-0,3295571	0,1472637	-2,24	0,025	-0,6181886	-0,0409255
NVWA	-0,1563875	0,1443105	-1,08	0,279	-0,4392309	0,1264560
RVO	-0,4761377	0,1426316	-3,34	0,001	-0,7556905	-0,1965848
age_group						
age 26_35	0,2590705	0,1889004	1,37	0,170	-0,1111675	0,6293085
age 36_35	0,6107770	0,1808975	3,38	0,001 ²⁵	0,2562244	0,9653297
age 46_35	0,8932088	0,1794323	4,98	0,000	0,5415280	1,2448900
age 55+	0,8957437	0,1809253	4,95	0,000	0,5411366	1,2503510
_cons						
Number of obs = 10929						
LR chi2(13) = 304,37						
Prob > chi2 = 0,0000						
Pseudo R2 = 0,0242						

Table A.4.8. PM: Regression analysis- overview Wald- χ^2 test results: Participants clicked on the embedded link

	Information	Experience	Combined
Control	$\chi^2=24,32$; P=0,000***	$\chi^2=45,72$; P=0,000***	$\chi^2=42,86$; P=0,000***
Information		$\chi^2=2,60$; P=0,107 ²⁶	$\chi^2=1,87$; P=0,172
Experience			$\chi^2= 0,07$; P=0,798 ²⁷

*P<0,10, **P<0,05, *** P<0,01 (With the NVWA included)

²⁵ With NVWA included significant (P<0,01); without significant (P<0,05)

²⁶ With NVWA included insignificant (P>0,10); without significant (P<0,01)

²⁷ With NVWA included insignificant (P>0,10); without significant (P<0,05)

Table A.4.9. PM: Logistic regression results, with participants filled in their password as independent variable (with the NVWA included)

M2_Password LOGIT	Coef.	Std. Err.	z	P>z	95% Confidence Interval	
1.male	0,1274494	0,0582439	2,19	0,029 ²⁸	0,0132935	0,2146053
1.Int_Employee	0,0004003	0,0824558	-0,00	0,996	-0,1620107	0,1612101
Group						
Information treatment	-0,3783161	0,0739847	-5,11	0,000	-0,5233234	-0,2333087
Experience treatment	-0,5519016	0,0737180	-7,49	0,000	-0,6963862	-0,4074171
Combined treatment	-0,6342530	0,0745428	-8,51	0,000	-0,7803543	-0,4881517
d_organisatieonderdeel						
DICTU	-0,6727303	0,1781228	-3,78	0,000	-1,0218440	-0,3236161
KD	-0,4985685	0,1648153	-3,03	0,002	-0,8216006	-0,1755364
NVWA	-0,3038699	0,1604407	-1,89	0,058	-0,6183279	-0,0105882
RVO	-0,6132715	0,1590636	-3,36	0,000	-0,9250304	-0,3015126
age_group						
age 26_35	0,3834965	0,2633521	1,46	0,145	-0,1326642	0,8996573
age 36_35	0,7869432	0,2525312	3,12	0,002 ²⁹	0,2919911	1,2818950
age 46_35	1,1854050	0,2502402	4,74	0,000 ³⁰	0,6949432	1,6758670
age 55+	1,3170040	0,2514457	5,24	0,000	0,8241798	1,8098290
_cons	-1,8968760	0,3009846	-6,30	0,000	-2,4867950	-1,3069580
Number of obs = 10929						
LR chi2(13) = 319,74						
Prob > chi2 = 0,0000						
Pseudo R2 = 0,0331						

Table A.4.10. PM: Regression analysis- overview Wald- χ^2 test results: participants filled in password

	Information	Experience	Combined
Control	$\chi^2=26,15$; P=0,000***	$\chi^2=56,05$; P=0,000***	$\chi^2=72,40$; P=0,000***
Information		$\chi^2=4,68$; P=0,031* ³¹	$\chi^2= 9,93$; P= 0,002*** ³²
Experience			$\chi^2= 1,04$; P=0,307

*P<0,10, **P<0,05, *** P<0,01

(With the NVWA included)

²⁸ With NVWA included significant (P<0,05); without insignificant (P>0,10)

²⁹ With NVWA included significant (P<0,01); without insignificant (P>0,10)

³⁰ With NVWA included significant (P<0,01); without significant (P<0,05)

³¹ With NVWA included significant (P<0,10); without significant (P<0,01)

³² With NVWA included significant (P<0,01); without significant (P<0,05)

Appendix 4.2. PM: Kruskal-Wallis test results (without the NVWA)

Table A.4.11. PM: Kruskal-Wallis equality-of-populations rank test: Age_Group

Group	Obs	Rank Sum
1 ³³	1803	7,02e+06
2	2203	8,03e+06
3	1986	7,34e+06
4	2002	7,68e+06

Chi-squared = 26,179
Probability = 0,0001

Chi-squared with ties = 28,172
Probability 0,0001

Table A.4.12. PM: Kruskal-Wallis equality-of-populations rank test: Age

Group	Obs	Rank sum
1	1803	7,58e+06
2	2203	8,45e+06
3	1986	7,79e+06
4	2002	8,13e+06

Chi-squared = 28,645
Probability = 0,0001

Chi-squared with ties = 28,666
Probability 0,0001

Table A.4.13. PM: Kruskal-Wallis equality-of-populations rank test: Gender

Group	Obs	Rank sum
1	1803	7,32e+06
2	2203	8,61e+06
3	1986	7,93e+06
4	2002	8,10e+06

Chi-squared = 5,544
Probability = 0,1360

Chi-squared with ties = 7,643
Probability 0,0540

Table A.4.14. PM: Kruskal-Wallis equality-of-populations rank test: Int_Employee

Group	Obs	Rank sum
1	1803	6,99e+06
2	2203	8,92e+06
3	1986	8,03e+06
4	2002	8,02e+06

Chi-squared = 6,822
Probability = 0,0778

Chi-squared with ties = 11,620
Probability 0,0088

Table A.4.15. PM: Kruskal-Wallis equality-of-populations rank test: Organizational subdivision

Group	Obs	Rank sum
1	1803	7,15e+06
2	2203	8,75e+06
3	1986	8,27e+06
4	2002	7,79e+06

Chi-squared = 15,274
Probability = 0,0016

Chi-squared with ties = 18,158
Probability 0,0004

³³ Group 1 = control; Group 2 = Information; Group 3 = Experience; Group 4 = Combined

Appendix 4.3. PM: M2_VisitLinkBIN: Logit regression analysis

Table A.4.16. PM: Logistic regression results. Y= participants clicked the embedded link (without the NVWA)

Y= M2_VisitLinkBIN	Coef.	Std. Err.	z	P>z	95% Confidence Interval	
1.male	0,1625823	0,0574995	2,83	0,005	0,0498852	0,2752793
1.Int_Employee	0,1539165	0,0695294	2,21	0,027	0,0176414	0,2901916
Group						
Control	-0,4192304	0,0750427	-5,59	0,000	-0,5663114	-0,2721494
Information	-0,6668600	0,0767750	-8,69	0,000	-0,8173362	-0,5163838
Experience	-0,5017927	0,0742725	-6,76	0,000	-0,6473640	-0,3562213
d_organisatieonderdeel						
<i>DICTU</i>	-0,3387355	0,1581487	-2,14	0,032	-0,6487012	-0,0287699
<i>KD</i>	-0,3266030	0,1498675	-2,18	0,029	-0,6203379	-0,0328681
<i>RVO</i>	-0,4812390	0,1445894	-3,33	0,001	-0,7646290	-0,1978491
age_group						
<i>age 26_35</i>	0,2174719	0,2430501	0,89	0,371	-0,2588976	0,6938414
<i>age 36_35</i>	0,4887898	0,2363413	2,07	0,039	0,0255693	0,9520103
<i>age 46_35</i>	0,8090855	0,2359068	3,44	0,001	0,3467167	1,271454
<i>age 55+</i>	0,7633267	0,2384863	3,20	0,001	0,2959021	1,230751
<i>_cons</i>						
Number of obs =		7994				
LR chi2(12) =		214,14				
Prob > chi2 =		0,0000				
Pseudo R2 =		0,0241				

Appendix 4.4. PM: M2_VisitLinkBIN: Wald- χ^2 test results and Fischer exact and χ^2 -test results (gender & employee contract).

Table A.4.17. PM: Overview Wald- χ^2 test results of the differences between organizational units of the number of participants who clicked on the embedded link in the phishing mail.

	DICTU	KD	RVO
AT	$\chi^2=4,59$; P = 0,032 **	$\chi^2=4,75$; P = 0,029 **	$\chi^2=11,08$; P= 0,001 ***
DICTU		$\chi^2=0,02$; P = 0,891	$\chi^2=3,12$; P= 0,078 *
KD			$\chi^2=6,16$; P= 0,013 **

*P<0,10, **P<0,05, *** P<0,01

Table A.4.18. PM: Overview Wald- χ^2 test results of the differences between age categories of the number of participants who clicked on the embedded link in the phishing mail.

	Age 26-35	Age 36-45	Age 46-55	Age 55+
Age 16-25	$\chi^2=0,80$; P= 0,371	$\chi^2=4,28$; P= 0,039**	$\chi^2=11,76$; P= 0,001***	$\chi^2=10,24$; P= 0,001***
Age 26-35		$\chi^2=7,93$; P= 0,005***	$\chi^2=38,99$; P= 0,000***	$\chi^2=29,70$; P= 0,000***
Age 36-45			$\chi^2=22,44$; P= 0,000***	$\chi^2=13,66$; P= 0,000***
Age 46-55				$\chi^2=0,43$; P= 0,514

*P<0,10, **P<0,05, *** P<0,01

Table A.4.19. PM: Fischer exact and chi2 test results – visiting the site : Gender

	Visited the site		
	No	Yes	Total
Female	2555	717	3272
Male	3492	1230	4722
Total	6047	1947	7994
Pearsons chi2(1)= 17,9377 Pr= 0,000			
Fischer's exact test= 0,000			
1-sided 0,000			

Table A.4.20. PM: Fischer exact and chi2 test results – visiting the site : Employee contract

	Visited the site		
	No	Yes	Total
External	2555	717	3272
Internal	3492	1230	4722
Total	6047	1947	7994
Pearsons chi2(1)= 16,4008 Pr= 0,000			
Fischer's exact test= 0,000			
1-sided 0,000			

Appendix 4.5. PM: M2_VisitLinkBIN: Correlation matrix

Table A.4.21. PM: Correlation matrix phishing mail experiment (Y=M2_VisitLinkBIN)

M2_VisitlinkBIN	<i>male</i>	<i>Int_ Employee</i>	<i>Information</i>	<i>Experience</i>	<i>Combined</i>	<i>DICTU</i>	<i>KD</i>	<i>RVO</i>	<i>age 26_35</i>	<i>age 36_35</i>	<i>age 46_35</i>	<i>age 55+</i>
<i>male</i>	1											
<i>Int_Employee</i>	0,0557	1										
<i>Information</i>	0,0098	-0,0456	1									
<i>Experience</i>	-0,0271	-0,0272	0,4487	1								
<i>Combined</i>	-0,0226	-0,0202	0,4593	0,4583	1							
<i>DICTU</i>	-0,0676	0,2234	0,2570	0,0239	0,0131	1						
<i>KD</i>	0,0586	0,0437	0,2887	-0,0169	-0,0237	0,8376	1					
<i>RVO</i>	0,0518	0,0737	0,2627	-0,0039	0,0023	0,8615	0,9111	1				
<i>age 26_35</i>	-0,0112	-0,0463	0,0128	0,0311	0,0247	0,0004	-0,0030	-0,0031	1			
<i>age 36_35</i>	-0,0203	-0,1216	0,0349	0,0371	0,0322	-0,0070	0,0054	0,0000	0,9196	1		
<i>age 46_35</i>	-0,0357	-0,1357	0,0407	0,0445	0,0335	-0,0023	0,0170	0,0086	0,9222	0,9590	1	
<i>age 55+</i>	-0,0753	-0,1483	0,0348	0,0424	0,0347	0,0069	-0,0008	0,0076	0,9137	0,9511	0,9563	1
<i>_cons</i>	-0,1181	-0,1316	-0,2872	-0,1441	-0,1423	-0,5008	-0,5083	-0,5232	-0,7669	-0,7856	-0,7889	-0,7741

Appendix 4.6. PM: M2_VisitLinkBIN: Variance Inflation Factor values

Table A.4.22. PM: VIF values phishing mail experiment

Variable	VIF	1/VIF
1.male	2,70	0,369858
1.Int_Employee	4,69	0,213138
Group		
<i>Information treatment</i>	2,13	0,469684
<i>Experience treatment</i>	2,05	0,488341
<i>Combined treatment</i>	2,06	0,485815
d_organisatieonderdeel		
<i>DICTU</i>	4,41	0,226553
<i>KD</i>	6,93	0,144395
<i>RVO</i>	10,69	0,093581
age_group		
<i>age 26_35</i>	4,28	0,233798
<i>age 36_35</i>	8,27	0,120859
<i>age 46_35</i>	8,50	0,117682
<i>age 55+</i>	6,97	0,143521
<u>Mean VIF</u>	<u>5,31</u>	

Appendix 4.7. PM: M2_Password: Logit regression analysis

Table A.4.23. PM: Logistic regression results. Y= participants filled in password (without the NVWA)

Y=M2_Password	Coef.	Std. Err.	z	P>z	95% Confidence Interval	
1.male	0,0401151	0,0695657	0,58	0,564	-0,0962311	0,1764614
1.Int_Employee	0,0485295	0,0850361	0,57	0,568	-0,1181381	0,2151971
Group						
<i>Information treatment</i>	-0,5700946	0,0891641	-6,39	0,000	-0,7448530	-0,3953362
<i>Experience treatment</i>	-0,8479609	0,0931801	-9,10	0,000	-1,0305910	-0,6653312
<i>Combined treatment</i>	-0,7266413	0,0898597	-8,09	0,000	-0,9027631	-0,5505195
d_organisatieonderdeel						
<i>DICTU</i>	-0,7171391	0,1815226	-3,95	0,000	-1,0729170	-0,3613614
<i>KD</i>	-0,5671941	0,1689926	-3,36	0,001	-0,8984207	-0,2359676
<i>RVO</i>	-0,6794963	0,1623772	-4,18	0,000	-0,9977498	-0,3612428
age_group						
<i>age 26_35</i>	0,0173695	0,2990400	0,06	0,954	-0,5687382	0,6034771
<i>age 36_35</i>	0,2539461	0,2897198	0,88	0,381	-0,3138943	0,8217865
<i>age 46_35</i>	0,6787823	0,2883720	2,35	0,019	0,1135835	1,2439810
<i>age 55+</i>	0,7944592	0,2909218	2,73	0,006	0,2242630	1,3646550
<i>_cons</i>	-1,186692	0,3351164	-3,54	0,000	-1,8435080	-0,5298762
<i>Number of obs = 7994</i> <i>LR chi2(12) = 220,17</i> <i>Prob > chi2 = 0,0000</i> <i>Pseudo R2 = 0,0330</i>						

Appendix 4.8. PM: M2_Password: Wald- χ^2 test results , Fischer exact and χ^2 -test results (gender & employee contract).

Table A.4.24. PM: Overview Wald-test χ^2 test results of the differences between organizations of the number of participants who filled in password

	DICTU	KD	RVO
AT	$\chi^2 = 4,59$; P = 0,032 **	$\chi^2 = 4,75$; P = 0,029 **	$\chi^2 = 11,08$; P = 0,001 ***
DICTU		$\chi^2 = 0,02$; P = 0,891	$\chi^2 = 3,12$; P = 0,078 *
KD			$\chi^2 = 6,16$; P = 0,013 **

*P<0,10, **P<0,05, *** P<0,01

Table A.4.25. PM: Overview Wald χ^2 test results of the differences between age categories in the number of participants who filled in password.

	Age 36-45	Age 46-55	Age 55+
Age 26-35	$\chi^2 = 3,68$; P = 0,055*	$\chi^2 = 30,47$; P = 0,000***	$\chi^2 = 38,17$; P = 0,000***
Age 36-45		$\chi^2 = 25,64$; P = 0,000***	$\chi^2 = 34,72$; P = 0,000***
Age 46-55			$\chi^2 = 2,11$; P = 0,147

*P<0,10, **P<0,05, *** P<0,01

Table A.4.26. PM: Fischer exact and chi2 test results – Filled in password: Gender

	Filled in password		
	No	Yes	Total
Female	2555	717	3272
Male	3492	1230	4722
Total	6047	1947	7994
Pearsons chi2(1)= 3,5035 Pr= 0,062			
Fischer's exact test= 0,061			
1-sided 0,033			

Table A.4.27. PM: Fischer exact and chi2 test results – visiting the site: Employee contract

	Filled in password		
	No	Yes	Total
External	2555	717	3272
Internal	3492	1230	4722
Total	6047	1947	7994
Pearsons chi2(1)= 10,4000 Pr= 0,001			
Fischer's exact test= 0,001			
1-sided 0,001			

Appendix 4.9. PM: M2_Password: Correlation matrix

Table A.4.28. PM: Correlation matrix phishing mail experiment

	<i>male</i>	<i>Int_ Employee</i>	<i>Information</i>	<i>Experience</i>	<i>Combined</i>	<i>DICTU</i>	<i>KD</i>	<i>RVO</i>	<i>age 26_35</i>	<i>age 36_35</i>	<i>age 46_35</i>	<i>age 55+</i>
<i>male</i>	1											
<i>Int_Employee</i>	0,0557	1										
<i>Information</i>	0,0119	-0,0446	1									
<i>Experience</i>	-0,0267	-0,0199	0,3959	1								
<i>Combined</i>	-0,0229	-0,0162	0,4063	0,3982	1							
<i>DICTU</i>	-0,0699	0,2385	0,2897	0,0294	0,0180	1						
<i>KD</i>	0,0677	0,0453	0,3282	-0,0182	-0,0251	0,8067	1					
<i>RVO</i>	0,0591	0,0823	0,3025	-0,0035	0,0020	0,8343	0,8974	1				
<i>age 26_35</i>	-0,0145	-0,0503	0,0142	0,0305	0,0255	-0,0004	-0,0030	-0,0026	1			
<i>age 36_35</i>	-0,0242	-0,1262	0,0388	0,0365	0,0327	-0,0081	0,0071	0,0020	0,9115	1		
<i>age 46_35</i>	-0,0401	-0,1414	0,0442	0,0437	0,0333	-0,0044	0,0122	0,0108	0,9168	0,9576	1	
<i>age 55+</i>	-0,0796	-0,1542	0,0375	0,0404	0,0334	0,0048	-0,0007	0,0088	0,9103	0,9517	0,9600	1
<i>_cons</i>	-0,1156	-0,1297	-0,2901	-0,1313	-0,1290	-0,4662	-0,4789	-0,4966	-0,7800	-0,8029	-0,8082	-0,7944

Appendix 4.10. PM: M2_Password: Variance Inflation Factor values

Table A.4.29. PM: VIF values phishing mail experiment

Variable	VIF	1/VIF
1.male	2,70	0,369858
1.Int_Employee	4,69	0,213138
Group		
<i>Information treatment</i>	2,13	0,469684
<i>Experience treatment</i>	2,05	0,488341
<i>Combined treatment</i>	2,06	0,485815
d_organisatieonderdeel		
<i>DICTU</i>	4,41	0,226553
<i>KD</i>	6,93	0,144395
<i>RVO</i>	10,69	0,093581
age_group		
<i>age 26_35</i>	4,28	0,233798
<i>age 36_35</i>	8,27	0,120859
<i>age 46_35</i>	8,50	0,117682
<i>age 55+</i>	6,97	0,143521
<i>Mean VIF</i>	5,31	

Appendix 4.11. SL: Differences in number of observations, average- and total pure working time

Table A.4.30. SL: Average pure working time, number of observations and total pure working time disaggregated per treatment group and time period

Group	Average pure working time per day per PC				Observations				Total pure working time			
	P1	P2	P3	P4 ³⁴	P1	P2	P3	P4	P1	P2	P3	P4
Control	5,058	4,951	4,962	5,080	4958	3493	3457	3440	25076,30	172943,38	17152,59	17474,13
Information	5,162	5,133	5,080	5,194	6086	4385	4334	4325	31416,61	22506,20	22018,23	22463,41
Reminders	5,179	5,066	5,126	5,177	4306	3070	3115	2995	22299,74	15553,61	15968,53	15504,98
Combined	5,197	4,993	4,966	5,084	4945	3535	3550	3435	25699,52	17649,13	17628,91	17464,48
<i>Average</i>	<i>5,149</i>	<i>5,041</i>	<i>5,034</i>	<i>5,136</i>	<i>5073,75</i>	<i>3620,75</i>	<i>3614</i>	<i>3548,75</i>	<i>26123,04</i>	<i>18250,83</i>	<i>18192,06</i>	<i>18226,75</i>

³⁴ P1 = pre-test period; P2 = Intervention period; P3 = short-term post-test period (2 weeks after the intervention period); P4= long-term post-test (3 months after the intervention period).

Appendix 4.12. SL: T-test results Per2-Per3, Per2-Per4 and Per3-Per4 comparison of number of times participants manually locked their screen per hour, and the ratio of manual locks to total locks.

Table A.4.31. SL: T-test results; Number of times of manually locked screens. The intervention period, compared to the short-term post-test and long-term post-test period, and short-term post-test and long-term post-test comparison, per treatment group.

Group	Period 2 – Period 3	Period 2 – Period 4	Period 3 – Period 4
Control	t=-0,761; P= 0,447	t=-0,198; P= 0,843	t= 0,579; P= 0,562
Information	t= 0,057; P= 0,955	t= 0,795; P= 0,427	t= 0,739; P= 0,460
Reminders	t= 0,152; P= 0,879	t= 1,215; P= 0,224	t= 1,045; P= 0,296
Combined	t= 0,639; P= 0,523	t= 2,428; P= 0,015**	t= 1,812; P= 0,070*

*P<0,10, **P<0,05, *** P<0,01

Table A.4.32. SL: T-test results, ratio manual locks to total locks. The intervention period, compared to the short-term post-test and long-term post-test period, and short-term post-test and long-term post-test comparison, per treatment group.

Group	Period 2 – Period 3	Period 2 – Period 4	Period 3 – Period 4
Control	t=-0,959; P= 0,338	t=-1,408; P= 0,159	t=-0,451; P= 0,652
Information	t=-0,438; P= 0,662	t=-0,379; P= 0,705	t= 0,058; P= 0,954
Reminders	t= 0,229; P= 0,819	t=-0,317; P= 0,751	t=-0,542; P= 0,588
Combined	t= 1,603; P= 0,109	t= 2,252; P= 0,024**	t= 0,670; P= 0,503

*P<0,10, **P<0,05, *** P<0,01

Appendix 4.13. SL: Main model: Hausman test results

Table A.4.33. SL: Hausman test result of the main model (fixed random, sigmamore)

	Coefficients			
	(b) Fixed	(B) Random	(b-B) Difference	$\sqrt{\text{diag}(V_b - V_B)}$ S.E.
dPeriode2 ³⁵	-0,0032758	-0,0064957	0,0032199	0,0016508
dPeriode3 ³⁶	0,0478287	0,0453224	0,0025063	0,0018329
dPeriode4 ³⁷	0,0407418	0,0383421	0,0023997	0,0019753
Per2G2 ³⁸	0,4812048	0,4769568	0,0042480	0,0021035
Per2G3 ³⁹	0,4197263	0,4169837	0,0027426	0,0022095
Per2G4 ⁴⁰	0,6977069	0,6920065	0,0057004	0,0021431
Per3G2	0,3972912	0,3950027	0,0022884	0,0024353
Per3G3	0,3779070	0,3735624	0,0043446	0,0025364
Per3G4	0,5353950	0,5284464	0,0069487	0,0024865
Per4G2	0,3489732	0,3457934	0,0031798	0,0028889
Per4G3	0,3498901	0,3477468	0,0021433	0,0027536
Per4G4	0,4276564	0,4237163	0,0039401	0,0026925
zuiverewerktijd ⁴¹	-0,0318167	-0,0360297	0,0042130	0,0007014
Tuesday	-0,0389275	-0,0435577	0,0046302	0,0008542
Wednesday	-0,1065091	-0,0839014	-0,0226077	0,0030438
Thursday	-0,0034517	-0,0007281	-0,0027236	0,0007540
Friday	-0,3801908	-0,3435462	-0,0366445	0,0056535
Usedpcoftotalpc ⁴²	0,7489539	0,8664341	-0,1174802	0,0181620

b = consistent under H_0 and H_a ; obtained from xtreg

B = inconsistent under H_a , efficient under H_0 ; obtained from xtreg

Test: H_0 : difference in coefficients not systematic

$$\begin{aligned} \chi^2(18) &= (b-B)'[(V_b - V_B)^{-1}](b-B) \\ &= 151,76 \end{aligned}$$

$$\text{Prob} > \chi^2 = 0,000$$

³⁵ Dperiod2 /Per2 =intervention period

³⁶ Dperiod3 /Per3= short-term post-test period

³⁷ Dperiod4 /Per4= long-term post-test period

³⁸ G2 = Treatment 1 (information provision by flyers)

³⁹ G3 = Treatment 2 (constant salient reminders)

⁴⁰ G4 = Treatment 3 (combined treatment)

⁴¹ Zuiverewerktij /Time = pure working time (Time computer logged on – time computer locked)

⁴² Usedpcoftotalpc/ usedpc = fraction of used computer of total computer per hallway

Appendix 4.14. SL: Main model: Correlation matrix

Table A.4.34. SL: Correlation matrix for the variables of the main model

e(V)	Per2	Per3	Per4	Per2G2	Per2G3	Per2G4	Per3G2	Per3G3	Per3G4	Per4G2	Per4G3	Per4G4	Time
Per2	1												
Per3	0,4173	1											
Per4	0,4157	0,4160	1										
Per2G2	-0,7417	-0,3071	-0,3063	1									
Per2G3	-0,6799	-0,2816	-0,2809	0,5092	1								
Per2G4	-0,7067	-0,2927	-0,2921	0,5290	0,4847	1							
Per3G2	-0,3072	-0,7410	-0,3067	0,4183	0,2111	0,2193	1						
Per3G3	-0,2819	-0,6817	-0,2816	0,2131	0,4196	0,2026	0,5096	1					
Per3G4	-0,2925	-0,7069	-0,2922	0,2206	0,2021	0,4170	0,5281	0,4873	1				
Per4G2	-0,3056	-0,3060	-0,7411	0,4182	0,2108	0,2190	0,4178	0,2121	0,2196	1			
Per4G3	-0,2805	-0,2808	-0,679	0,2102	0,4152	0,2001	0,2097	0,4177	0,2005	0,5063	1		
Per4G4	-0,2920	-0,2923	-0,7061	0,2182	0,1999	0,4136	0,2178	0,2008	0,4152	0,5259	0,4812	1	
Time	0,0091	0,0096	0,0018	-0,0021	0,0024	0,0068	-0,0020	-0,0023	0,0070	-0,0003	-0,0003	0,0046	1
Tue	0,0077	0,0082	0,0041	0,0027	0,0018	0,0026	0,0012	0,0007	0,0036	0,0034	0,0009	0,0012	0,0241
Wed	-0,0289	-0,0274	-0,0289	-0,0145	-0,0141	-0,0117	-0,0083	-0,0223	-0,0154	-0,0130	-0,0052	-0,0005	0,0056
Thur	-0,0018	-0,0009	-0,0052	-0,0018	-0,0001	-0,0027	0,0003	-0,0015	0,0005	0,0005	0,0005	-0,0001	0,0354
Fri	-0,0446	-0,042	-0,0405	-0,0228	-0,017	-0,0163	-0,0109	-0,0280	-0,0228	-0,0215	-0,0091	-0,0024	0,0369
usedpc	-0,0576	-0,0565	-0,0503	-0,0325	-0,0255	-0,023	-0,0167	-0,0367	-0,0313	-0,0284	-0,0115	-0,0033	0,0092
_cons	0,0000	-0,0014	-0,004	0,0297	0,0224	0,0193	0,0150	0,0346	0,0266	0,0252	0,0102	0,0015	-0,3037

	Tue	Wed	Thur	Fri	usedpc
Tue	1				
Wed	0,3507	1			
Thur	0,4958	0,4208	1		
Fri	0,2220	0,6056	0,3241	1	
usedpc	-0,1018	0,5081	0,0410	0,7224	1
_cons	-0,0480	-0,5798	-0,1820	-0,7574	-0,9269

Appendix 4.15. SL: Main model: Variance Inflation Factor values

Table A.4.35. SL: VIF values of variables in the main model

Variable	VIF	1/VIF
<i>Usedpcoftotalpc</i>	11,17	0,089547
<i>zuiverewerktijd</i>	7,67	0,130362
<i>dPeriode3</i>	4,95	0,202220
<i>dPeriode2</i>	4,94	0,202349
<i>dPeriode4</i>	4,88	0,204852
<i>Per2G2</i>	2,27	0,440332
<i>Per4G2</i>	2,27	0,441451
<i>Per3G2</i>	2,25	0,444860
<i>Tuesday</i>	2,03	0,492513
<i>Per3G4</i>	2,03	0,493087
<i>Per2G4</i>	2,02	0,495247
<i>Per4G4</i>	2,00	0,500590
<i>Thursday</i>	1,90	0,525506
<i>Per3G3</i>	1,90	0,525624
<i>Per2G3</i>	1,88	0,531876
<i>Per4G3</i>	1,86	0,536713
<i>Wednesday</i>	1,58	0,631265
<i>Friday</i>	1,41	0,709693
<i>Mean VIF</i>	3,28	

Appendix 4.16. *SL*: Main model: Autocorrelation and heteroscedasticity tests

Table A.4.36. *SL*: Wooldridge test for autocorrelation in panel data: Extended model

H0:	No first order autocorrelation
	F(1,1716)= 22,839
	Prob>F= 0,0000

Table A.4.37. *SL*: Modified Wald test for groupwise heteroskedasticity: Extended model

H0:	$\sigma(i)^2 = \sigma^2$ for all i
	Chi2 (1812)= 5,4e+06
	Prob>F= 0,0000

Appendix 4.17. SL: Main model: Fixed effects regression analysis

Table A.4.38. SL: Fixed effects regression results. Y= number of times participants manually locked their screen

Fixed-effects (within) regression					Number of observations =	62751
with Driscoll-Kraay standard errors					Number of groups =	1812
Group variable: DstringPC						
R-sq: within =	0,0167				Obs per group: min =	1
R-sq: within =	0,0167				Avg =	33,4
					Max =	45
					F =	112,90
Variable	Coef.	Std. Err.	T	P>t	95% Conf. Interval	
dgroup2		0 (omitted)				
dgroup3		0 (omitted)				
dgroup4		0 (omitted)				
dPeriode2	0,0130841	0,0404033	0,32	0,748	-0,0683434	0,0945116
dPeriode3	0,0533207	0,0448265	1,19	0,241	-0,0370213	0,1436626
dPeriode4	0,0504586	0,0479818	1,05	0,299	-0,0462423	0,1471595
Per2G2	0,4770422	0,0699547	6,82	0,000	0,3360577	0,6180267
Per2G3	0,3900288	0,0337061	11,57	0,000	0,3220986	0,4579590
Per2G4	0,6644686	0,0507017	13,11	0,000	0,5622861	0,7666511
Per3G2	0,3773355	0,0976437	3,86	0,000	0,1805476	0,5741235
Per3G3	0,3710629	0,0526787	7,04	0,000	0,2648959	0,4772299
Per3G4	0,5184991	0,0699261	7,41	0,000	0,3775724	0,6594258
Per4G2	0,3435538	0,0864253	3,98	0,000	0,1693751	0,5177325
Per4G3	0,3257633	0,0615450	5,29	0,000	0,2017274	0,4497991
Per4G4	0,4024621	0,0609259	6,61	0,000	0,2796742	0,5252501
zuiverewerktijdu	0,0351890	0,0105700	3,33	0,000	0,0138866	0,0564914
Tuesday	-0,0229707	0,0268926	-0,85	0,398	-0,0771692	0,0312278
Wednesday	-0,1103663	0,0373415	-2,96	0,005	-0,1856232	-0,0351094
Thursday	-0,0069827	0,0458492	0,15	0,880	-0,0854203	0,0993857
Friday	-0,3776343	0,0583127	-6,48	0,000	-0,4951558	-0,2601128
usedpcoftotalpc	0,8316339	0,1835597	4,53	0,000	0,4616937	1,2015740
_cons	1,4256870	0,1414954	10,08	0,000	1,1405220	1,7108520

Appendix 4.18. SL: Main model: Wald-test results

Table A.4.39. SL: Treatment impact comparison in the intervention period

	Reminder treatment	Combined treatment
Information treatment	F= 1,58; P= 0,215	F= 25,35; P= 0,000 ***
Reminder treatment		F= 33,00; P= 0,000 ***

*P<0,10, **P<0,05, *** P<0,01

Table A.4.40. SL: Treatment impact comparison in the short-term post-test period

	Reminder treatment	Combined treatment
Information treatment	F= 0,01; P= 0,928	F= 9,54; P= 0,004 ***
Reminder treatment		F= 8,24; P= 0,006 ***

*P<0,10, **P<0,05, *** P<0,01

Table A.4.41. SL: Treatment impact comparison in the long-term post-test period

	Reminder treatment	Combined treatment
Information treatment	F= 0,03; P= 0,853	F= 1,59; P= 0,214
Reminder treatment		F= 1,06; P= 0,308

*P<0,10, **P<0,05, *** P<0,01

Table A.4.42. SL: Treatment impact comparison of Per2-Per3, Per2-Per4 and Per3-Per4

Group	Period 2 – Period 3	Period 2 – Period 4	Period 3 – Period 4
Information	F= 1,57; P= 0,217	F= 6,05; P= 0,018 **	F= 0,19; P= 0,690
Reminder	F= 0,09; P= 0,760	F= 0,85; P= 0,361	F= 0,30; P= 0,587
Combined	F= 6,27; P= 0,016 **	F=29,93; P= 0,000 ***	F= 3,35; P= 0,074

*P<0,10, **P<0,05, *** P<0,01

Appendix 4.19. SL: Extended model: Hausman test results

Table A.4.43. SL: Hausman test result of the extended model (fixed random, sigmamore)

	Coefficients		(b-B) Difference	sqrt(diag(V_b-V_B)) S,E,
	(b) Fixed	(B) Random		
dPeriode2	-0,148420	-0,147750	-0,000670	0,005668
dPeriode3	-0,130940	-0,137620	0,006679	0,005544
dPeriode4	-0,021300	-0,026880	0,005577	0,006553
Per2G2	0,579969	0,577089	0,002880	0,007156
Per2G3	0,243312	0,242040	0,001272	0,007867
Per2G4	0,454365	0,449900	0,004465	0,008237
Per3G2	0,448853	0,449588	-0,000730	0,007712
Per3G3	0,496216	0,498035	-0,001820	0,008119
Per3G4	0,203776	0,210902	-0,007130	0,008223
Per4G2	0,418024	0,421777	-0,003750	0,010239
Per4G3	0,243733	0,243210	0,000523	0,010296
Per4G4	0,192401	0,193002	-0,000600	0,009435
Per2Time ⁴³	0,031664	0,031067	0,000598	0,001035
Per3Time	0,036216	0,037133	-0,000920	0,001004
Per4Time	0,014003	0,014764	-0,000760	0,001223
Per2G2Time ⁴⁴	-0,020450	-0,020800	0,000343	0,001316
Per2G3Time	0,026488	0,026241	0,000247	0,001460
Per2G4Time	0,040880	0,040673	0,000208	0,001483
Per3G2Time	-0,014050	-0,014780	0,000732	0,001371
Per3G3Time	-0,025360	-0,026600	0,001236	0,001493
Per3G4Time	0,061928	0,059445	0,002483	0,001470
Per4G2Time	-0,014810	-0,016220	0,001411	0,001826
Per4G3Time	0,015233	0,014656	0,000577	0,001876
Per4G4Time	0,040162	0,039419	0,000743	0,001742
G2Time	0,043689	0,047564	-0,003870	0,001815
G3Time	-0,066360	-0,061630	-0,004730	0,001986
G4Time	-0,004700	-0,000390	-0,004310	0,001915
zuiverewerktijd	0,013521	0,007247	0,006274	0,001354
Tuesday	-0,025140	-0,029970	0,004829	0,000746
Wednesday	-0,110660	-0,089310	-0,021340	0,002926
Thursday	0,005854	0,007923	-0,002070	0,000636
Friday	-0,376160	-0,340970	-0,035190	0,005471
Usedpcoftotalpc	0,839950	0,954915	-0,114960	0,017555

Test: H0: difference in coefficients not systematic

$$\begin{aligned} \chi^2(18) &= (b-B)'[(V_b-V_B)^{-1}](b-B) \\ &= 169,28 \\ \text{Prob}>\chi^2 &= 0,000 \end{aligned}$$

⁴³ Per2Time = interaction term of period 2 (intervention period) with zuiverewerktijd/ Time (average pure working time)

⁴⁴ Per2G2Time = interaction term of period 2 (intervention period), group 2 (treatment 1) and zuiverewerktijd/Time

Appendix 4.20. SL: Extended model: Correlation matrix (3 parts)

Table A.4.44. SL: Correlation matrix for the variables of the main model

e(V) (1/3)	Per2	Per3	Per4	Per2G2	Per2G3	Per2G4	Per3G2	Per3G3	Per3G4	Per4G2	Per4G3	Per4G4
Per3	0,4102	1										
Per4	0,3993	0,4025	1									
Per2G2	-0,7418	-0,3040	-0,2960	1								
Per2G3	-0,6861	-0,2812	-0,2738	0,5094	1							
Per2G4	-0,7124	-0,2920	-0,2843	0,5291	0,4892	1						
Per3G2	-0,3067	-0,7483	-0,3010	0,4149	0,2106	0,2187	1					
Per3G3	-0,2806	-0,6852	-0,2756	0,2086	0,4141	0,2004	0,5131	1				
Per3G4	-0,2940	-0,7177	-0,2887	0,2186	0,2020	0,4208	0,5375	0,4924	1			
Per4G2	-0,2945	-0,2969	-0,7381	0,3986	0,2022	0,2101	0,4060	0,2036	0,2134	1		
Per4G3	-0,2760	-0,2782	-0,6918	0,2050	0,4055	0,1969	0,2084	0,4090	0,1999	0,5109	1	
Per4G4	-0,2837	-0,2860	-0,7113	0,2108	0,1949	0,4051	0,2143	0,1963	0,4122	0,5253	0,4924	1
Per2Time	-0,9260	-0,3758	-0,3658	0,6874	0,6356	0,6601	0,2813	0,2576	0,2698	0,2701	0,2531	0,2602
Per3Time	-0,3750	-0,9248	-0,3685	0,2785	0,2574	0,2674	0,6924	0,6341	0,6643	0,2721	0,2550	0,2622
Per4Time	-0,3671	-0,3706	-0,9291	0,2727	0,2521	0,2618	0,2775	0,2542	0,2663	0,6860	0,6431	0,6612
Per2G2Time	0,6947	0,2820	0,2745	-0,9266	-0,4769	-0,4953	-0,3810	-0,1932	-0,2025	-0,3662	-0,1899	-0,1953
Per2G3Time	0,6436	0,2612	0,2543	-0,4776	-0,9253	-0,4587	-0,1955	-0,379	-0,1874	-0,1877	-0,3707	-0,1808
Per2G4Time	0,6633	0,2692	0,2620	-0,4924	-0,4554	-0,9253	-0,2015	-0,1845	-0,3832	-0,1935	-0,1813	-0,3690
Per3G2Time	0,2838	0,6998	0,2788	-0,3803	-0,1948	-0,2023	-0,9240	-0,4797	-0,5025	-0,3725	-0,1929	-0,1984
Per3G3Time	0,2612	0,6442	0,2567	-0,1939	-0,3798	-0,1862	-0,4822	-0,9248	-0,4626	-0,1895	-0,3754	-0,1826
Per3G4Time	0,2709	0,6681	0,2662	-0,2012	-0,1806	-0,3827	-0,5002	-0,4581	-0,9231	-0,1966	-0,1842	-0,3754
Per4G2Time	0,2735	0,2760	0,6916	-0,3666	-0,1876	-0,1948	-0,3736	-0,1890	-0,1981	-0,9303	-0,4785	-0,4920
Per4G3Time	0,2575	0,2599	0,6515	-0,1911	-0,3727	-0,1836	-0,1946	-0,3765	-0,1866	-0,4810	-0,9270	-0,4636
Per4G4Time	0,2624	0,2650	0,6645	-0,1951	-0,1803	-0,3706	-0,1985	-0,1819	-0,3775	-0,4907	-0,4600	-0,9284
G2Time	-0,4155	-0,4214	-0,4108	0,5565	0,2851	0,2961	0,5705	0,2887	0,3025	0,5496	0,2842	0,2922
G3Time	-0,3848	-0,3902	-0,3805	0,2857	0,5581	0,2744	0,2922	0,5627	0,2803	0,2810	0,5530	0,2708
G4Time	-0,3974	-0,4031	-0,3931	0,2951	0,2729	0,5628	0,3019	0,2765	0,5774	0,2903	0,2721	0,5573



Time	0,5568	0,5648	0,5507	-0,4134	-0,3822	-0,3970	-0,4229	-0,3872	-0,4056	-0,4066	-0,3811	-0,3918
Tue	-0,0051	-0,0079	-0,0053	0,0092	0,0018	0,0038	0,0069	0,0015	0,0093	0,0097	-0,0002	0,0043
Wed	-0,0180	-0,0121	-0,0083	0,0006	0,0037	-0,0031	0,0014	-0,0087	-0,0058	0,0029	-0,005	-0,0070
Thur	-0,0054	-0,0050	-0,0026	0,0068	0,0055	0,0034	0,0077	-0,0022	0,0060	0,0104	0,0002	0,0052
Fri	-0,0203	-0,0160	-0,0128	-0,0038	0,0012	-0,0047	-0,0037	-0,0096	-0,0083	-0,0014	-0,0042	-0,0050
usedp	-0,0225	-0,0195	-0,0151	-0,0092	-0,0012	-0,0081	-0,0021	-0,0117	-0,0130	-0,0031	-0,0043	-0,0085

e(V) (2/3)	Per2Time	Per3Time	Per4Time	Per2G2T	Per2G3T	Per2G4T	Per3G2T	Per3G3T	Per3G4T	Per4G2T	Per4G3T	Per4G4T	G2Time
Per2Time	1												
Per3Time	0,4020	1											
Per4Time	0,3932	0,3966	1										
Per2G2Time	-0,7502	-0,3016	-0,2950	1									
Per2G3Time	-0,6949	-0,2793	-0,2732	0,5214	1								
Per2G4Time	-0,7164	-0,2880	-0,2817	0,5374	0,4978	1							
Per3G2Time	-0,3041	-0,7565	-0,3000	0,4081	0,2114	0,2179	1						
Per3G3Time	-0,2799	-0,6964	-0,2762	0,2100	0,4067	0,2005	0,5269	1					
Per3G4Time	-0,2904	-0,7224	-0,2865	0,2179	0,2018	0,4073	0,5465	0,5031	1				
Per4G2Time	-0,2927	-0,2952	-0,7442	0,3932	0,2034	0,2097	0,4003	0,2056	0,2133	1			
Per4G3Time	-0,2757	-0,2781	-0,7012	0,2068	0,3984	0,1975	0,2104	0,4042	0,2009	0,5218	1		
Per4G4Time	-0,2812	-0,2837	-0,7152	0,2110	0,1953	0,3940	0,2146	0,1975	0,4013	0,5322	0,5015	1	
G2Time	0,4448	0,4507	0,4430	-0,5974	-0,3092	-0,3187	-0,611	-0,3139	-0,3257	-0,5923	-0,3106	-0,3169	1
G3Time	0,4121	0,4176	0,4105	-0,3092	-0,5965	-0,2953	-0,316	-0,6042	-0,3017	-0,3055	-0,5964	-0,2936	0,515
G4Time	0,4257	0,4314	0,4241	-0,3195	-0,2958	-0,5979	-0,3264	-0,3005	-0,6135	-0,3156	-0,2974	-0,5971	0,5322
Time	-0,5964	-0,6044	-0,5941	0,4475	0,4144	0,4273	0,4573	0,4209	0,4366	0,4421	0,4165	0,4248	-0,7455
Tue	0,0086	0,0120	0,0076	-0,0087	-0,0018	-0,0032	-0,0070	-0,0014	-0,0090	-0,0089	0,0003	-0,0045	0,0064
Wed	0,0078	0,0023	-0,0018	-0,0063	-0,0094	-0,0013	-0,0051	0,0001	-0,0002	-0,0082	0,0026	0,0067	0,0028
Thu	0,0053	0,0050	0,0010	-0,0081	-0,0061	-0,0044	-0,0082	0,0017	-0,0061	-0,0110	-0,0002	-0,0054	0,0112
Fri	0,0040	0,0005	-0,0019	-0,0050	-0,0081	-0,0013	-0,0012	-0,0015	-0,0002	-0,0071	0,0001	0,0044	0,0014
usedp	0,0006	-0,0020	-0,0036	-0,0027	-0,0081	-0,0001	-0,0045	-0,0024	0,0018	-0,0077	-0,0004	0,0079	0,0089

e(V) (3/3)	G3Time	G4Time	Time	Tue	Wed	Thur	Fri	usedp
G3Time	1							
G4Time	0,4930	1						
Time	-0,6906	-0,7135	1					
Tue	0,0075	0,0016	-0,0035	1				
Wed	-0,0013	-0,0096	0,0060	0,3538	1			
Thur	0,0044	0,0052	0,0059	0,4962	0,4245	1		
Fri	-0,0018	-0,0026	0,0161	0,2248	0,6079	0,3281	1	
usedpc	-0,0004	-0,0007	-0,0007	-0,1022	0,5050	0,0411	0,7225	1

Appendix 4.21. SL: Extended model: Variance Inflation Factor values

Table A.4.45. SL: VIF values of variables of the extended model (1/2)

Variable	VIF	1/VIF
Per4Time	37,31	0,026802
Per2Time	35,93	0,027829
Per3Time	35,61	0,028079
Per4	34,47	0,029007
Per2	33,07	0,030235
Per3	32,54	0,03073
Time	27,93	0,035806
Per4G2Time	18,95	0,052776
Per2G2Time	18,06	0,055371
Per4G2	17,07	0,058576
Per3G2Time	17,06	0,058628
Usedpc	17,05	0,058638
Per2G2	15,96	0,062654
Per4G4Time	15,89	0,062939
Per2G4Time	15,19	0,06582
Per3G2	15	0,066665
Per4G3Time	14,92	0,067042
Per3G3Time	14,73	0,067876
Per4Time	37,31	0,026802

(2/2)

Per3G4Time	14,7	0,068009
Per2G3Time	14,53	0,068826
Per4G4	14,48	0,069069
Per2G4	13,83	0,072321
Per3G4	13,28	0,075281
Per4G3	13,28	0,075307
Per2G3	12,95	0,077236
Per3G3	12,94	0,077253
G2Time	7,08	0,141185
G4Time	6,14	0,16286
G3Time	5,9	0,16947
Tuesday	2,03	0,491974
Thursday	1,92	0,521593
Wednesday	1,66	0,603162
<i>Mean VIF</i>	<i>16,76</i>	

Appendix 4.22. *SL*: Extended model: Autocorrelation and heteroscedasticity tests

Table A.4.46. *SL*: Wooldridge test for autocorrelation in panel data: Extended model

H0:	No first order autocorrelation
	F(1,1716)= 22,735
	Prob>F= 0,0000

Table A.4.47. *SL*: Modified Wald test for groupwise heteroskedasticity: Extended model

H0:	$\sigma(i)^2 = \sigma^2$ for all i
	Chi2 (1812)= 4,9e+06
	Prob>F= 0,0000

Appendix 4.23. SL: Extended model: Fixed effects regression analysis

Table A.4.48. SL: Fixed effects regression results, with the number of times participants manually locked their screen as independent variable – Extended model

<i>Variable</i>	<i>Coef.</i>	<i>Std. Err.</i>	<i>T</i>	<i>P>t</i>	<i>95% Conf. Interval</i>	
Fixed-effects (within) regression with					Number of observations =	62751
Driscoll-Kraay standard errors					Number of groups =	1812
					Obs per group: min =	1
Group variable: DstringPC					Avg =	33,4
R-sq: within = 0,0178					Max =	45
					F =	535,41
<i>Variable</i>	<i>Coef.</i>	<i>Std. Err.</i>	<i>T</i>	<i>P>t</i>	<i>95% Conf. Interval</i>	
dPeriode2	-0,1484165	0,0700734	-2,12	0,040	-0,2896401	-0,0071929
dPeriode3	-0,1309364	0,0781513	-1,68	0,101	-0,2884399	0,0265672
dPeriode4	-0,0212992	0,1291418	-0,16	0,870	-0,2815675	0,2389690
Per2G2	0,5799692	0,1933481	3,00	0,004	0,1903016	0,9696367
Per2G3	0,2433124	0,1215911	2,00	0,052	-0,0017384	1,4883631
Per2G4	0,4543649	0,1141088	3,98	0,000	0,2243937	1,6843361
Per3G2	0,4488531	0,1792453	2,50	0,016	0,0876080	0,8100983
Per3G3	0,4962157	0,1433221	3,46	0,001	0,2073690	1,7850624
Per3G4	0,2037758	0,2033205	1,00	0,322	-0,2059898	0,6135415
Per4G2	0,4180237	0,1650518	2,53	0,015	0,0853838	0,7506636
Per4G3	0,2437332	0,1145386	2,13	0,039	0,0128959	1,4745705
Per4G4	0,1924014	0,1319425	1,46	0,152	-0,0735113	0,4583141
Per2Time	0,0316640	0,0161510	1,96	0,056	-0,0008861	0,0642142
Per3Time	0,0362157	0,0187228	1,93	0,060	-0,0015176	0,0739491
Per4Time	0,0140028	0,0255307	0,55	0,586	-0,0374510	0,0654565
Per2G2Time	-0,0204541	0,0302128	-0,68	0,502	-0,0813440	0,0404358
Per2G3Time	0,0264880	0,0203622	1,30	0,200	-0,0145493	0,0675252
Per2G4Time	0,0408801	0,0246990	1,66	0,105	-0,0088974	0,0906576
Per3G2Time	-0,0140497	0,0257664	-0,55	0,588	-0,0659785	0,0378791
Per3G3Time	-0,0253634	0,0270432	-0,94	0,353	-0,0798655	0,0291387
Per3G4Time	0,0619282	0,0415497	1,49	0,143	-0,0218097	0,1456661
Per4G2Time	-0,0148130	0,0229915	-0,64	0,523	-0,0611493	0,0315233
Per4G3Time	0,0152329	0,0218583	0,70	0,490	-0,0288196	0,0592855
Per4G4Time	-0,0401616	0,0274090	1,47	0,150	-0,0150777	0,0954008
Zuiverewerktijd	0,0135207	0,0168725	0,80	0,427	-0,0204835	0,0475249
G2Time	0,0316640	0,0165191	2,64	0,011	0,0130967	0,769810
G3Time	0,0362157	0,0190101	-3,49	0,001	-0,1046710	-0,0280462
G4Time	0,0140028	0,0217688	-0,22	0,830	-0,0485726	0,0391719
Tuesday	-0,0251416	0,0262794	-0,96	0,344	-0,0781042	0,0278211
Wednesday	-0,1106577	0,0371137	-2,98	0,005	-0,1854555	-0,0358598
Thursday	-0,0058539	0,0447087	0,13	0,896	-0,0842507	0,0959584
Friday	-0,3761561	0,0575088	-6,54	0,000	-0,4920574	-0,2602547
usedpcoftotalpc	0,8399504	0,1824277	-4,60	0,000	0,4722916	1,207609
_cons	1,5438740	0,1483680	10,41	0,000	1,2448570	1,842890

Appendix 4.24. SL: Extended model: Wald-test results.

Table A.4.49. SL: Treatment impact comparison in the intervention period

	Reminder treatment	Combined treatment
Information treatment	F= 1,61; P= 0,212	F= 19,15; P= 0,000 ***
Reminder treatment		F= 32,05; P= 0,000 ***

*P<0,10, **P<0,05, *** P<0,01

Table A.4.50. SL: Treatment impact comparison in the short-term post-test period

	Reminder treatment	Combined treatment
Information treatment	F= 0,02; P= 0,883	F= 7,06; P= 0,011 **
Reminder treatment		F= 7,47; P= 0,009 ***

*P<0,10, **P<0,05, *** P<0,01

Table A.4.51. SL: Treatment impact comparison in the long-term post-test period

	Reminder treatment	Combined treatment
Information treatment	F= 0,03; P= 0,858	F= 1,26; P= 0,264
Reminder treatment		F= 0,86; P= 0,359

*P<0,10, **P<0,05, *** P<0,01

Table A.4.52. SL: Treatment impact comparison of Per2-Per3, Per2-Per and Per3-Per4

Group	Period 2 – Period 3	Period 2 – Period 4	Period 3 – Period 4
Information	F= 1,45; P= 0,235	F= 5,93; P= 0,019 **	F= 0,21; P= 0,649
Reminder	F= 0,03; P= 0,867	F= 0,54; P= 0,467	F= 0,23; P= 0,634
Combined	F= 6,93; P= 0,012 **	F= 30,70; P= 0,000 ***	F= 3,57; P= 0,065

*P<0,10, **P<0,05, *** P<0,01

Bibliography

- Adams, J.G.U. (1983). Public Safety legislation and the risk compensation hypothesis: the example of motorcycle helmet legislation. *Environment and Planning*, 1(2), 193-203.
- Adams, J. (1999). Cars, Cholera and Cows: the management of risk and uncertainty. *Policy Analysis*, (335), 1-49.
- Ajzen, I. (2012). Martin Fishbein's legacy the reasoned action approach. *The Annals of the American Academy of Political and Social Science*, 640(1), 11-27.
- Alberts, H.J., Martijn, C., & de Vries, N.K. (2011). Fighting self-control failure: overcoming ego depletion by increasing self-awareness. *Journal of Experimental Social Psychology*, 47(1), 58-62.
- Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, 26(4), 276-289.
- Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security*, 28(6), 476-490.
- Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, 29(4), 432-445.
- Auditdienst Rijk. (2014). *Rapport onderzoek beveiligingskennis van EZ-medewerkers*. Den Haag: Ministerie van Financiën.
- Aurigemma, S., & Panko, R. (2012). A composite framework for behavioral compliance with information security policies. In *proceedings of the 45th Hawaii International Conference on System Science (HICSS)* (pp. 3248-3257). Maui: IEEE.
- Bada, M., Sasse, A., & Nurse, J. (2014). *Cyber security awareness campaigns: Why do they fail to change behavior?*. Global Cyber Security Centre.
- Baker, E. M., Baker, W.H., & Tedesco, J.C. (2007). Organizations respond to phishing: Exploring the public relations tackle box. *Communication Research Reports*, 24(4), 327-339.
- Berghel, H. (2006). Phishing mongers and posers. *Communications of the ACM*, 49(4), 21-25.
- Berkowitz, A.D. (2005). An overview of the social norms approach. In L. Lederman, & L. Stewart, *Changing the culture of college drinking: A socially situated health communication campaign* (pp. 193-214). New York: Hampton Press.
- Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. *Computers and Security*, 23(3), 253-264.
- Blythe, M., Petrie, H., & Clark, J. A. (2011). F for fake: four studies on how we fall for phish. In *proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 3469-3478). New York: ACM.
- Bowen, B.M., Devarajan, R., & Stolfo, S. (2011). Measuring the human factor of cyber security. In *proceedings of the IEEE International Conference on Technologies for Homeland Security (HST)* (pp. 230-235). IEEE.

- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3), 523-548.
- Burns, M.B., Durcikova, A., & Jenkins, J. L. (2013). What kind of interventions can help users from falling for phishing attempts: a research proposal for examining stage-appropriate interventions. In *proceedings of the 46th Hawaii International Conferences on System Sciences (HICSS)* (pp. 4023-4032). IEEE.
- Calzolari, G., & Nardotto, M. (2011). Nudging with information: A randomized field experiment on reminders and feedback. Working paper, University of Bologna.
- Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy and Security*, 1(3), 18-41.
- Charles, T., Quinn, D., Weatherall, M., Aldington, S., Beasley, R., & Holt, S. (2007). An audiovisual reminder function improves adherence with inhaled corticosteroid therapy in asthma. *Journal of Allergy and Clinical Immunology*, 119(4), 811-816.
- Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, 39, 447-459.
- Choi, M. S. (2013). Assessing the role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills toward computer misuse intention at government agencies. Nova Southeastern University.
- D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, 20(1), 79-98.
- Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behavior among internet users. *Computers in human behavior*, 26(6), 1739-1747.
- D'Egidio, G., Patel, R., Rashidi, B., Mansour, M., Sabri, E., & Milgram, P. (2014). A study of the efficacy of flashing lights to increase the salience of alcohol-gel dispensers for improving hand hygiene compliance. *American journal of infection control*, 42(8), 852-855.
- Demakis, J.G., Beauchamp, C., Cull, W.L., Denwood, R., Eisen, S.A., Lofgren, R., & Henderson, W.G. (2000). Improving residents' compliance with standards of ambulatory care: results from the VA cooperative study on computerized reminders. *Jama*, 284(11), 1411-1416.
- Dhamija, R., Tygar, J.D., & Hearst, M. (2006). Why phishing works. In *proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 581-590). Montréal: ACM.
- Dhillon, G. (1999). Managing and Controlling Computer Misuse. *Information Management & Computer Security*, 7(4), 171-175.
- Dodge, R.C., Carver, C., & Ferguson, A.J. (2007). Phishing for user security awareness. *Computers & Security*, 26(1), 73-80.
- Downs, J.S., Holbrook, M.B., & Cranor, L.F. (2006). Decision strategies and susceptibility to phishing. In *proceedings of the Second symposium on Usable privacy and security* (pp. 79-90). Pittsburgh: ACM.

- Downs, J.S., Holbrook, M.B., & Cranor, L.F. (2007). Behavioral response to phishing risk. In *proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (pp. 37-44). Pittsburgh: ACM.
- Ferguson, A.J. (2005). Fostering e-mail security awareness: The west point carronade. *Educase Quarterly*, 28(1), 54-57.
- Furnell, S. (2007). Phishing: Can we spot the signs? *Computer Fraud & Security*, (3), 10-15.
- Garner, R. (2005). Post-it persuasion: a sticky influence. *Journal of Consumer Psychology*, 15(3), 230-237.
- Gerrard, M., Gibbons, F.X., & Reis-Bergan, M. (1998). The effect of risk communication on risk perceptions : the significance of individual differences. *Journal of the National Cancer Institute. Monographs*, (25), 94-100.
- Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A.P., Mundie, D., & Cowley, J. (2014). Analysis of unintentional insider threats deriving from social engineering exploits. In *proceedings of the 2014 IEEE Security and Privacy Workshops (SPW)* (pp. 236-250). Washington: IEEE .
- Hasvold, P.E., & Wootton, R. (2011). Use of telephone and SMS reminders to improve attendance at hospital appointments: a systematic review. *Journal of telemedicine and telecare*, 17(7), 358-364.
- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106-125.
- Hermesen, S., Frost, J., Renes, R.J., & Kerkhof, P. (2016). Using feedback through digital technology to disrupt and change habitual behavior: A critical review of current literature. *Computers in Human behavior*, 57, 61-74.
- Hoechle, D. (2007). Robust standard errors for panel regressions with cross-sectional dependence. *Stata Journal*, 7(3), 281.
- Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: the critical role of top management and organizational culture. *Decision sciences*, 43(4), 615-660.
- Ifinedo, P. (2011). Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory. *Computers & Security*, 31(1), 83-95.
- Jagatic, T.N., Johnson, N.A., & Menczer, F. (2007). Social Phishing. *Communications of the ACM*, 50(10), 94-100.
- Just, D.R., & Wansink, B. (2009). Smarter lunchrooms: Using behavioral economics to improve meal selection. *Choices*, 24(3), 1-7.
- Karlan, D., McConnell, M., Mullainathan, S., & Zinman, J. (2010). Getting to the top of mind: How reminders increase saving. *NBER Working Paper Series*.
- Kluger, A.N., & DeNisi, A. (1996). The effects of feedback interventions on performance: a historical review, a meta-analysis, and a preliminary feedback intervention theory. *Psychological bulletin*, 119(2), 254.
- Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L.F., Hong, J., Blair, M. A., & Pham, T. (2009). School of Phish: A Real-World Evaluation of Anti-Phishing Training. In *proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS '09)* (pp. 1-12). New York: ACM.

- Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L.F., Hong, J., & Nunge, E. (2007). Protecting people from phishing: the design and evaluation of an embedded training email system. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 905-914). New York: ACM.
- Lee, J., & Lee, Y. (2002). A Holistic Model of Computer Abuse within Organizations. *Information Management & Computer Security*, 10(2), 57-63.
- Leventhal, H., Benjamin, Y., Brownlee, S., Diefenbach, M., Leventhal, E.A., Patrick-Miller, L., & Robitaille, C. (1997). Illness representations : Theoretical foundations. In K. Petrie, & J. Weinman, *Perceptions of health and illness* (pp. 19-46). London: Hardwood Academic Publishers.
- Lewis, A.L., & Eves, F. F. (2012). Testing the theory underlying the success of point-of-choice prompts: A multi-component stair climbing intervention. *Psychology of Sport and Exercise*, 13(2), 126-132.
- Maurer, J., & Harris, K.M. (2014). Issuance of patient reminders for influenza vaccination by US-based primary care physicians during the first year of universal influenza vaccination recommendations. *American journal fo public health*, 104(6). e(60)-e(62).
- Merhi, M.I., & Midha, V. (2012). The impact of training and social norms on information security compliance: A pilot study. *Proceedings of the 33rd International Conference on Information Systems*. Orlando.
- Mohebzada, J.G., El Zarka, A., Bhojani, A. H., & Darwish, A. (2012). Phishing in a university community: two large scale phishing experiments. In *proceedings of the International Conference on Innovations in Information Technology (IIT)* (pp. 249-254). Abu Dhabi: IEEE.
- Nevo, I., Fitzpatrick, M., Thomas, R.E., Gluck, P.A., Lenchus, J.D., Arheart, K.L., & Birnbach, D.J. (2010). The efficacy of visual cues to improve hand hygiene compliance. *Simulation in Healthcare*, 5(6), 325-331.
- Notani, A.S. (1998). Moderators of perceived behavioral control's predictiveness in the theory of planned behavior: A meta-analysis. *Journal of Consumer Psychology*, 7(3), 247-271.
- Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. In *proceedings of the 40th Annual Hawaii International Conference on system sciences* (pp. 156b-156b). Waikoloa: IEEE.
- Painter, J.E., & Wansink, B. (2002). How visibility and convenience influence candy consumption. *Appetite*, 38(3), 237-238.
- Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013). Phishing for the truth: A scenario-based experiment of users' behavioural response to emails. In *proceedings of the 8th IFIP TC 11 International Conference, SEC 2013* (pp. 366-378). Auckland: Springer Berlin Heidelberg.
- Payne, S. (2003). Developing security education and awareness programs: Prevention in the form of education and awareness programs can help campuses avoid serious security ills. *Educause Quarterly*, 26(4), 49-53.
- Post, G. V., & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security*, 26(3), 229-237.

- Privitera, G.J., & Creary, H.E. (2013). Proximity and visibility of fruits and vegetables influence intake in a kitchen setting among college students. *Environment and Behavior*, 45(7), 876-886.
- Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 34(4), 758-778.
- PwC, CIO & CSO. (2015). *Global State of Information Security Survey 2015: Managing cyber risks in an interconnected world*. PwC.
- PWC, Cio & CSO. (2016). *Global State of Information Security Survey 2016: Turnaround and transformation in cybersecurity*. PwC.
- Raifman, J.R., Lanthorn, H.E., Rokicki, S., & Fink, G. (2014). The impact of text message reminders on adherence to antimalarial treatment in northern Ghana: a randomized trial. *PloS one*, 9(10).
- Ramanathan, V., & Wechsler, H. (2013). Phishing detection and impersonated entity discovery using conditionals random field and latent dirichlet allocation. *Computers & Security*, 34, 123-139.
- Rasbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information systems research*, 20(1), 121-139.
- Rogers, R. (1983). Cognitive and physiological processes in fear appeals and attitude change : A revised theory of protection motivation. In J. T. Cacioppo, *Social Psychophysiology: A Sourcebook* (pp. 153-177). New York: Guilford Press.
- Sheng, S., Kumaraguru, P., Acquisti, A., Cranor, L.F. & Hong, J.(2009). Improving phishing countermeasures: An analysis of expert interviews. *Proceedings of the 4th APWG eCrime Researchers Summit*, 2,4.
- Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In *proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 373-382). New York: ACM.
- Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J., & Nunge, E. (2007). Anti-phishing phill: the design and evaluation of a game that teaches people not to fall for phish. *The 3rd symposium on Usable privacy and security* (pp. 88-99). ACM.
- Siponen, M. T. (2000). Critical analysis of different approaches to minimizing user-related faults in information systems security: Implications for research and practice. *Information management & computer security*, 8(5), 197-209.
- Siponen, M.T., Pahlila, S., & Mahmood, M.A. (2006). A new model for understanding users' IS security compliance. *PACIS 2006 Proceedings. Paper 48*. PACIS.
- Siponen, M.T, Mahmood, M.A., & Pahlila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & management*, 51(2), 217-224.
- Smith, K., & Tobin, G. A. (1979). Human adjustment to the flood hazard. London: Longman.
- Straub, D. W., & Welke, R.J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, 4(22), 441-469.
- Svensson, M., Svensson, T., Hansen, A.W., & Lagerros, Y.T. (2012). The effect of reminders in a web-based intervention study. *European journal of epidemiology*, 27(5), 333-340.

- Taubinsky, D. (2014). From intentions to actions: a model and experimental evidence of inattentive choice. *Working paper*.
- Taylor, S., & Todd, P.A (1995). Understanding information technology usage: A test of competing models. *Information systems research*, 6(2), 144-176.
- Van Niekerk, J. F., & Von Solms, R. (2006). Understanding information security culture: a conceptual framework. In *Information Security South Africa (ISSA)*, (pp. 1-10). Johannesburg.
- Van Niekerk, J.F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, 29(4), 476-486.
- Venkatesh, V., & Davis, F.D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Managemtn science*, 46(2), 186-204.
- Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, 51(3), 576-586.
- Vogelsang, T. J. (2012). Heteroskedasticity, autocorrelation, and spatial correlation robust inference in linear panel models with fixed-effects. *Journal of Econometrics*, 166(2), 303-319.
- Vroom, C. V. (2004). Towards information security behavioural compliance. *Computers & Security*, 23(3), 191-198.
- Waly, N., Tassabehji, R., & Kamala, M. (2012). Improving organisational information security management: The impact of training and awareness. In *14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICES)*, (pp. 1270 - 1275). Liverpool: IEEE.
- Wansink, B., Painter, J.E., & Lee, Y.K. (2006). The office candy dish: Proximity's influence on estimated and actual consumption. *International journal of obesity*, 30(5), 871-875.
- Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, 18(2), 101-105.
- Warkentin, M., Carter, I., & McBride, M. (2012). Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. *Technical Report*, RTI International.
- Weinstein, N.D. (1989). Effects of personal experience on self-protective behavior. *Psychological bulletin*, 105(1), 31.
- Weinstein, N.D., & Sandman, P.M. (2002). The precaution adoption process model. In K. Glanz, B. K. Rimer, & F. M. Lewis, *Health behavior and health education: Theory, research and practice* (pp. 121-143). San-Francisco: Jossey-Bass.
- Whitman, M. (2004). In Defense of the Realm: Understanding the Threats to Information Security,. *International Journal of Information Management*, 24(1), 43-57.
- Whitman, M., & Mattord, H. (2003). *Principles of information security*. Kennesaw state university. Thomson course technology.
- Wilson, A.L., Bogomolova, S., & Buckley, J.D. (2015). Lack of efficacy of a salience nudge for substituting selection of lower-calorie for higher-calorie milk in the work place. *Nutrients*, 7(6), 4336-4344.

- Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health education & behavior*, 27(5), 591-615.
- Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems*, 27(1), 273-303.
- Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*, 330-340.
- Zurovac, D., Sudoi, R.K., Akhwale, W.S., Ndiritu, M., Hamer, D.H., Rowe, A.K., Snow, R.W. (2011). The effect of mobile phone text-message reminders on Kenyan health workers' adherence to malaria treatment guidelines: a cluster randomised trial. *The lancet*, 378(9793), 795-803.