UNIVERSITEIT TWENTE.

SOCIAL ENGINEERING

SUMMERSCHOOL 2019

MARIANNE JUNGER

M.JUNGER@UTWENTE.NL

WHY?
WHAT?
WHERE?
WHEN?
WHO?
HOW?
WHERE?
WHO?
HOW?
HOW?
WHAT? HOW? WHY?
WHO? WHERE? WHAT? HOW?
WHAT?
WHY? HOW? WHERE?
WHO? WHO?
WHO?
WHERE?
HOW? WHO?
WHO? WHERE? WHAT? HOW?
WHAT? HOW? WHY?
HOW?

CYBERCRIME

BRUCE SCHNEIER (2000) HTTPS://WWW.SCHNEIER.COM/

- ‘*Only amateurs attack machines; professionals target people*’

- *‘security is only as good as it’s weakest link, and people are the* ***weakest link*** *in the chain*.’

Schneier, B. (2000). Secrets and lies: digital security in a networked world. New York: John Wiley & Sons.

THE HUMAN IN THE LOOP

DEFINITION SOCIAL ENGINEERING:

ONLINE & OFFLINE FRAUD

Definition *'The science of using social interaction as a means to persuade an individual or an organization to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity'* *

* Mouton, F., Leenen, L., Malan, M. M., & Venter, H. S. (2014). Towards an Ontological Model Defining the Social Engineering Domain. In IFIP Advances in Information and Communication Technology (Vol. 431, pp. 266-279).)

WHY EXPLOIT ‘HUMAN AS THE ‘WEAKEST LINK’ IN SECURITY?

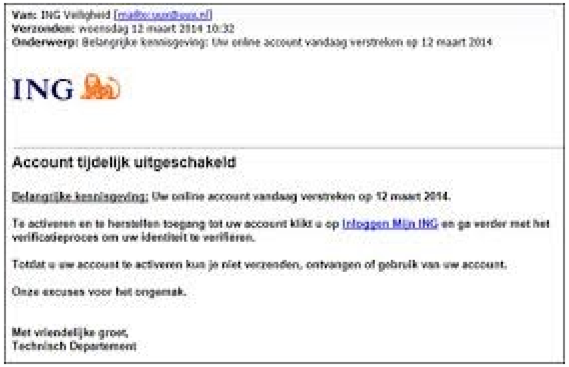
Easier

‘Invented’ by Kevin Mitnick

- https://www.youtube.com/watch?v=ScRl8Gudt-4
- https://www.youtube.com/watch?v=7YCOgcVgAIc
- https://www.youtube.com/watch?v=ZQDyCRHptbU

EXAMPLES OF SOCIAL ENGINEERING (SE)

Non technical way to hack a computer



Van: ING Veiligheid [mailto:[illegible]]
Verzonden: woensdag 12 maart 2014 10:32
Onderwerp: Belangrijke kennisgeving: Uw online account vandaag verstreken op 12 maart 2014

ING

Account tijdelijk uitgeschakeld

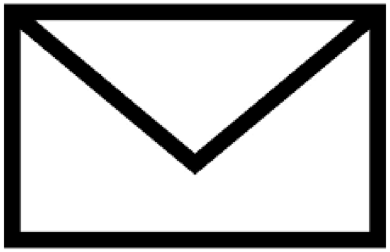
Belangrijke kennisgeving: Uw online account vandaag verstreken op 12 maart 2014.

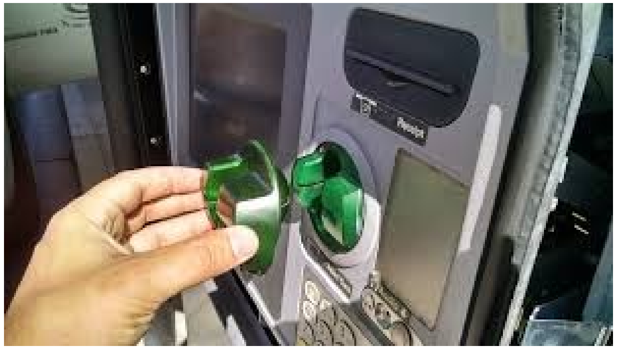
Te activeren en te herstellen toegang tot uw account klikt u op Inloggen Mijn ING en ga verder met het verificatieproces om uw identiteit te verifiëren.

Totdat u uw account te activeren kun je niet verzenden, ontvangen of gebruik van uw account.

Onze excuses voor het ongemak.

Met vriendelijke groet,
Technisch Departement





Important of non-technical attacks

Type of attacks, worldwide, according to Verizon

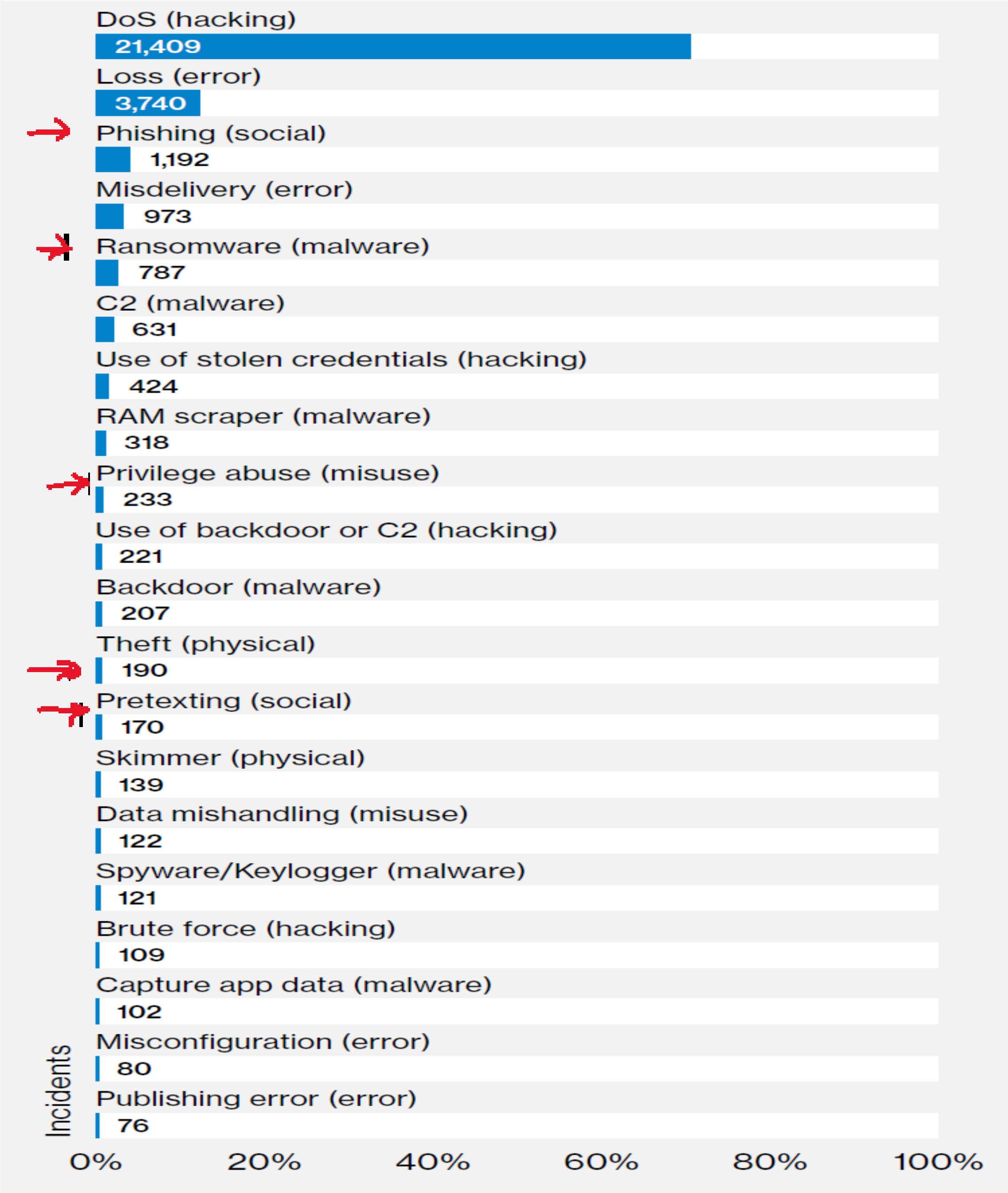


Figure 4. Top 20 threat action varieties (incidents) (n=30,362)

Verizon Risk Team. (2018). 2018 Data Breach Investigations Report. 11th edition. Retrieved from http://www.verizonenterprise.com/DBIR/2013
/

Social engineering studies at UT

Aims

- Study vulnerabilities of victims
- Prevention: can we help users against falling for SE attacks

“Can we get something from you – that would be useful to commit a crime?”

- **Key experiment**
- **Telephone-based social-engineering**
- **Questions for shoppers: ‘Can I get your bank account number?’**
- **Spear versus ‘traditional’ phishing emails**
- **Anti-phishing training**
- USB-Key experiment
- Anti-phishing training fro children

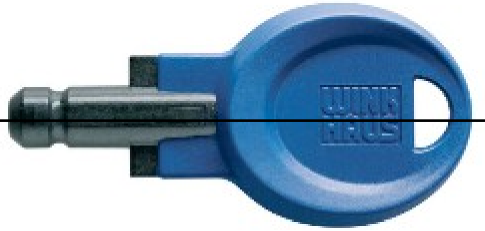
Face to Face: Door Key experiment

Can I have your key, please?

1. 118 rooms
2. Story ‘recharge key’

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. Journal of Experimental Criminology, 11(1), 97-115. doi: 10.1007/s11292-014-9222-7

Face to Face: Door Key experiment



Intentions

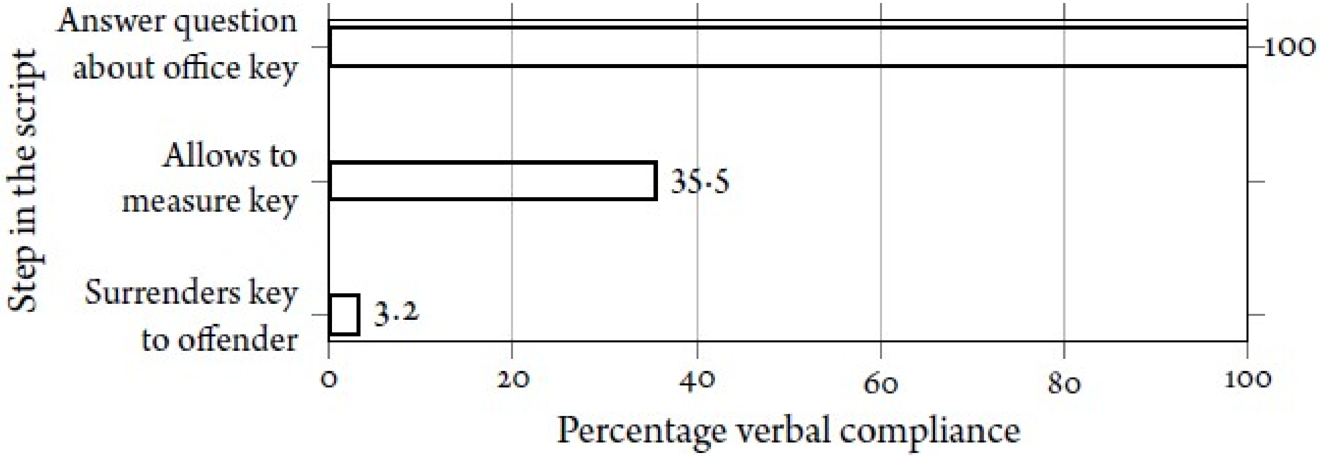


Figure 3.2: Intention to follow the instruction of the offender using F2F social engineering ($N = 31$)

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. Journal of Experimental Criminology, 11(1), 97-115. doi: 10.1007/s11292-014-9222-7

Face to Face, Door Key experiment.
In reality:

1. Compliance: 62.5%

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. Journal of Experimental Criminology, 11(1), 97-115. doi: 10.1007/s11292-014-9222-7

Telephone phishing

1. Frequent method to contact consumers (29.9% of all scams)*
2. ‘Attackers’ target 45 UT-staff
3. Story:
   - “your PC is sending spam,
   - You can download and execute a program that will remove the malware”

* National Consumer League
http://fraudresearchcenter.org/wp-content/uploads/2012/02/National-Consumers-League-2011-Top-Scams-of-2011.pdf
Bullee, J.-W., Montoya, L., Junger, M., & Hartel, P. (2016, 14-15 Jan 2016). *Telephone-based social*

Telephone phishing

Intentions

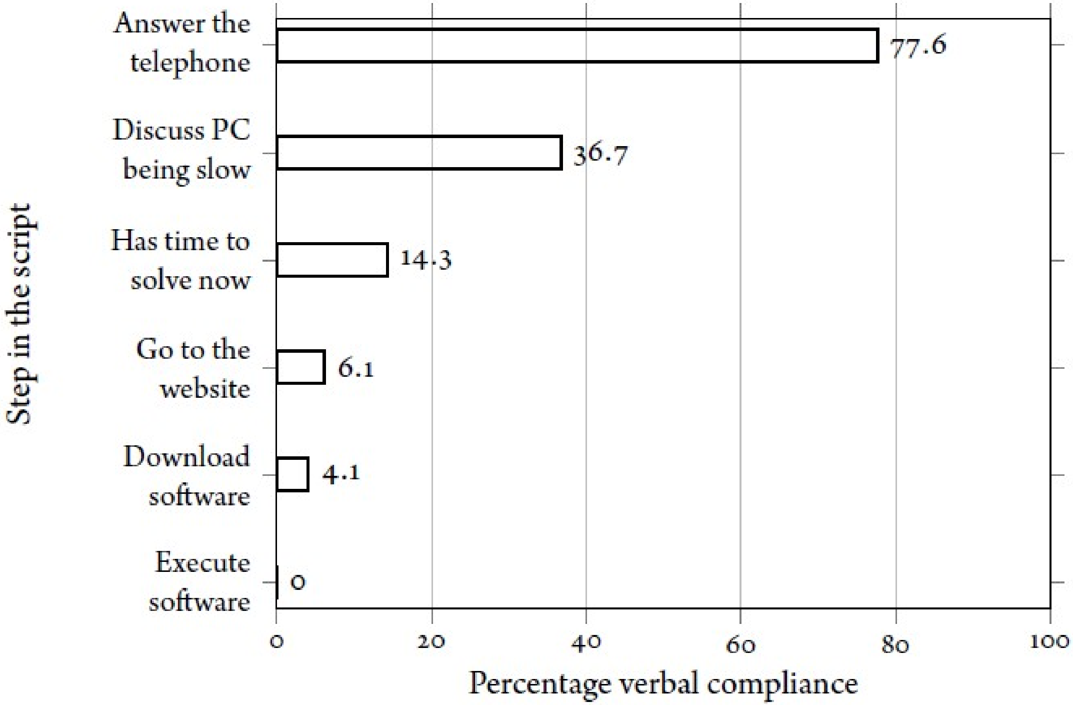


Figure 3.1: Intention to follow the instruction of the offender using telephone social engineering ($N = 49$)

Bullee, J.-W., Montoya, L., Junger, M., & Hartel, P. (2016, 14-15 Jan 2016). Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention. Paper presented at the Cyber Security R&D Conference (SG-CRC) 2016, Singapore.

Telephone phishing: in reality

40% downloaded the program

Bullee, J.-W., Montoya, L., Junger, M., & Hartel, P. (2016, 14-15 Jan 2016). Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention. Paper presented at the Cyber Security R&D Conference (SG-CRC) 2016, Singapore.

Questions for shoppers

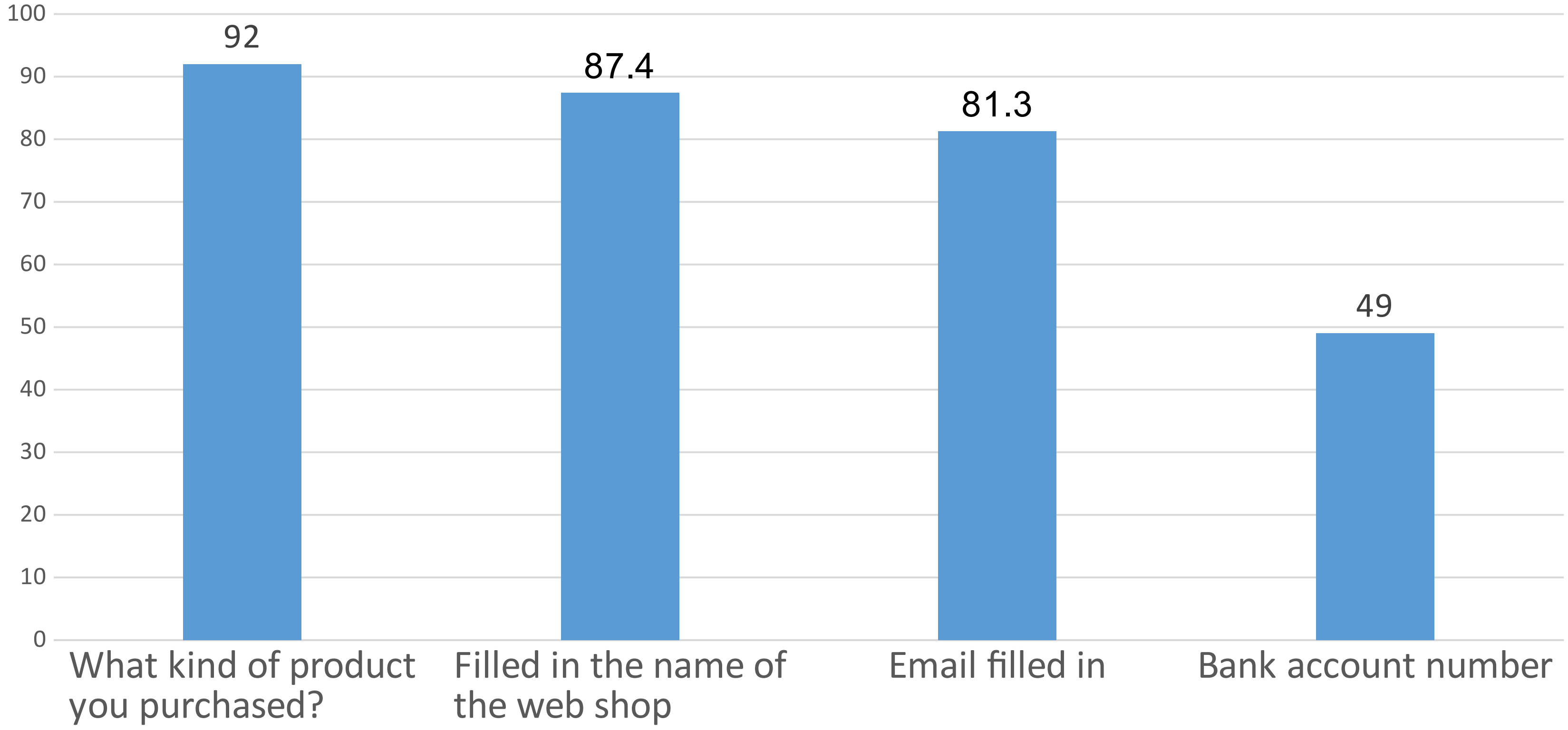
1. 278 questionnaires filled in in shopping area
2. 3 page questionnaire on cyber security
3. How easy is it to collect information for spear phishing?
   - Can you fill in your email address?
   - Bank account: □□ XX □□□□ XXXXXXX □□□

   Online shoppers only

   - What kind of product you purchased?
   - Filled in the name of the web shop

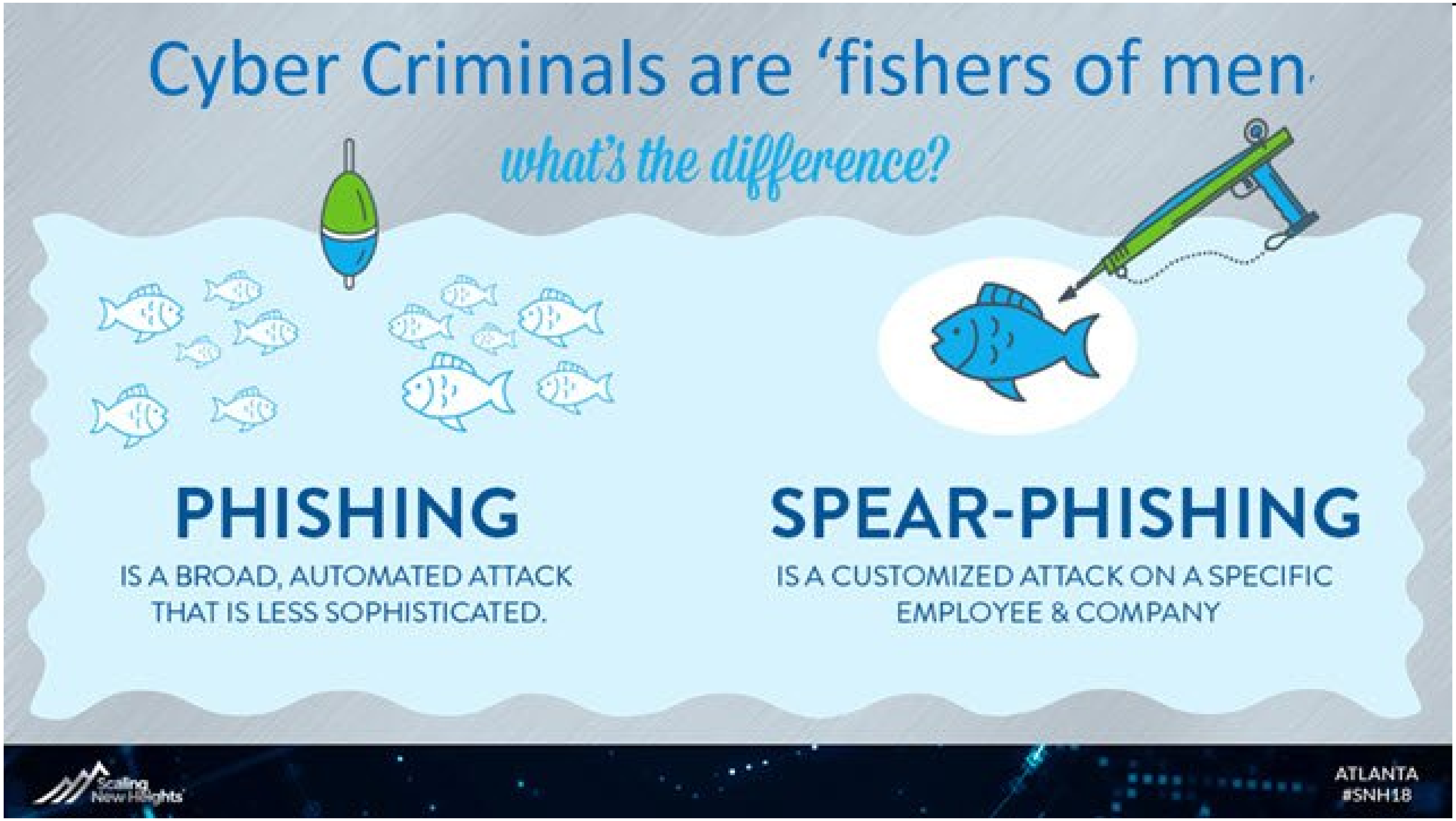
Junger, M., Montoya Morales, A. L., & Overink, F.-J. (2017). Priming and warnings are not effective to prevent social engineering attacks. Computers in Human Behavior, 66, 75-87.

Subjects providing personal identifiable information (PII) in %


100
90
80
70
60
50
40
30
20
10
0
92
87.4
81.3
49
What kind of product you purchased?
Filled in the name of the web shop
Email filled in
Bank account number

Junger, M., Montoya Morales, A. L., & Overink, F.-J. (2017). Priming and warnings are not effective to prevent social engineering attacks. Computers in Human Behavior, 66, 75-87.

SPEAR PHISHING


Cyber Criminals are 'fishers of men'
what's the difference?
PHISHING
IS A BROAD, AUTOMATED ATTACK THAT IS LESS SOPHISTICATED.
SPEAR-PHISHING
IS A CUSTOMIZED ATTACK ON A SPECIFIC EMPLOYEE & COMPANY
Scaling New Heights
ATLANTA
#SNH18

Bullee, J.-W., Montoya, L., Junger, M., & Hartel, P. (2017). Spear phishing in organisations explained. Information and Computer Security. doi: https://doi.org/10.1108/ICS-03-2017-0009

SPEAR PHISHING: PLAN

1. A faculty at the University of Twente - N=593
2. What was wrong:
   - Instead of www.utwente.nl -> www.UTvvente.nl
   - Sender 'Jort Welp', not an employee of the UT.
   - 'the IT help desk' called instead of 'ICTS'

3.Two conditions: General email 'dear employee'

Spear phishing 'dear Marianne Junger'

Bullee, J.-W., Montoya, L., Junger, M., & Hartel, P. (2017). Spear phishing in organisations explained. Information and Computer Security. doi: https://doi.org/10.1108/ICS-03-2017-0009

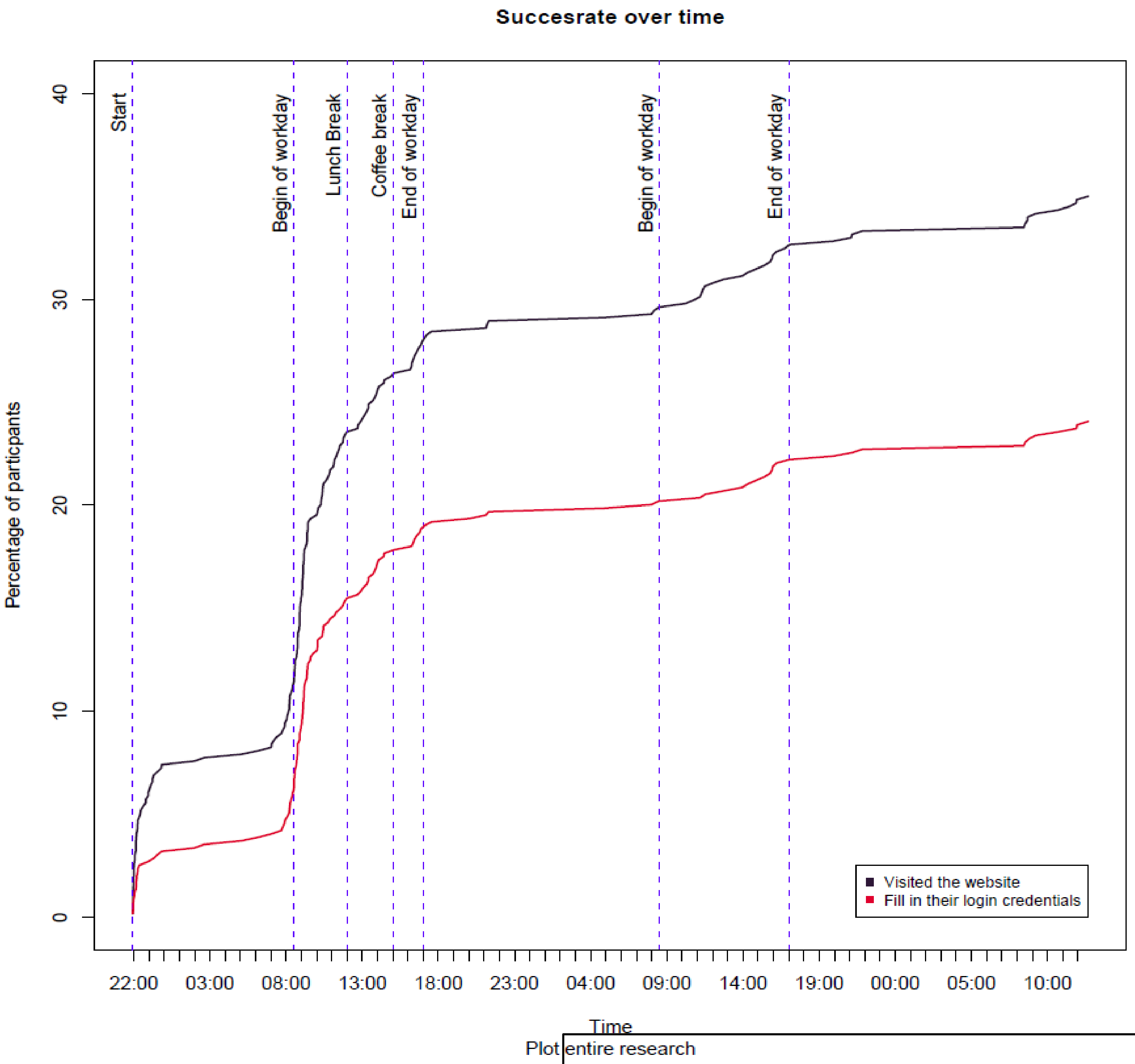
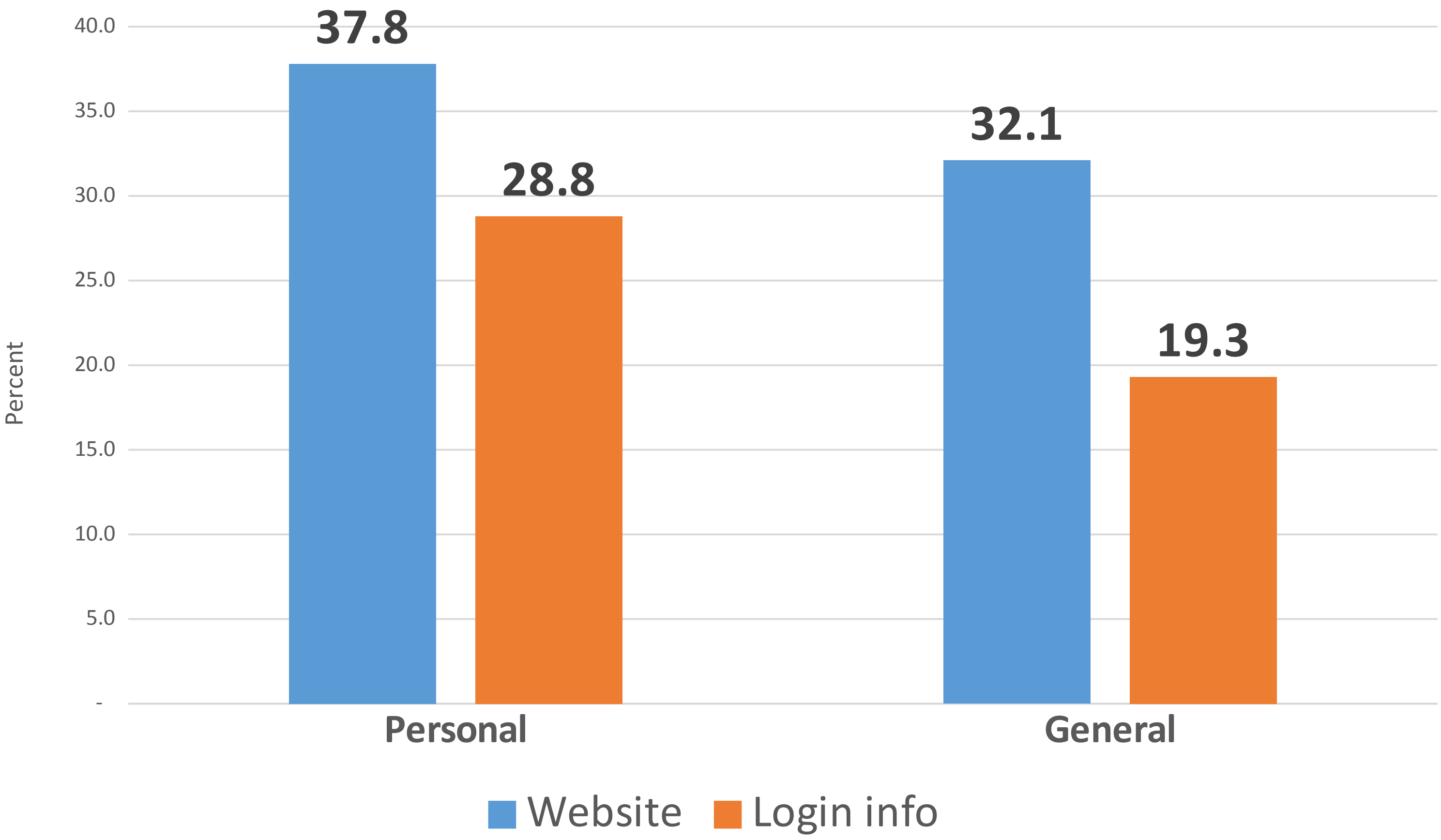


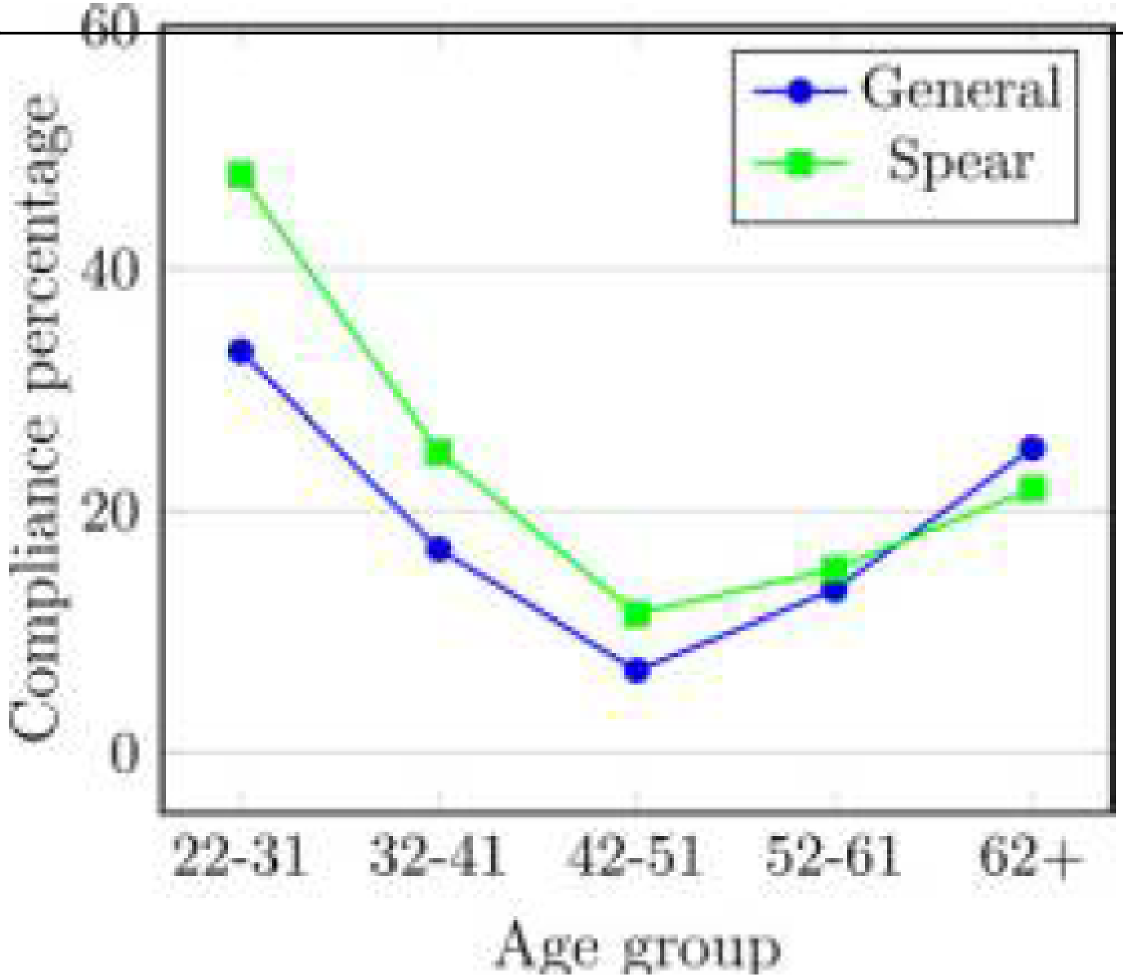
Figure 1: Unique site visits and login attempts over time.

SUCCESS RATE OF GENERAL AND SPEAR PHISHING EMAIL



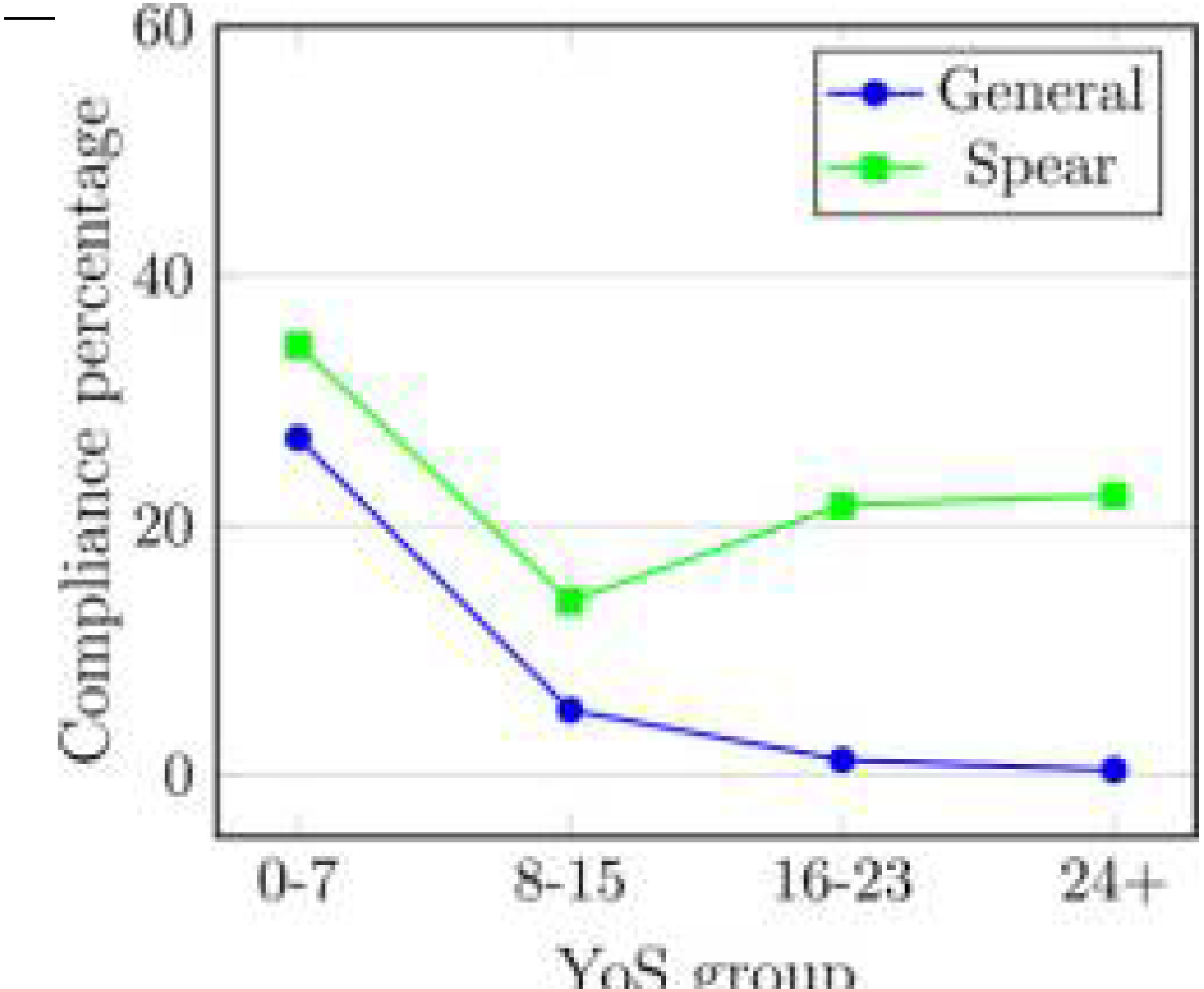
Bullee, J.-W., Montoya, L., Junger, M., & Hartel, P. (2017). Spear phishing in organisations explained. Information and Computer Security. doi: https://doi.org/10.1108/ICS-03-2017-0009

Success rate of general and spear phishing email by age



Bullee, J.-W., Montoya, L., Junger, M., & Hartel, P. (2017). Spear phishing in organisations explained. Information and Computer Security. doi: https://doi.org/10.1108/ICS-03-2017-0009

SUCCESS RATE OF GENERAL AND SPEAR PHISHING EMAIL BY AGE & YoS



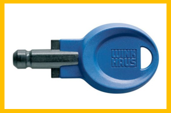
Bullee, J.-W., Montoya, L., Junger, M., & Hartel, P. (2017). Spear phishing in organisations explained. Information and Computer Security. doi: https://doi.org/10.1108/ICS-03-2017-0009

Spear phishing: who is most vulnerable?

	Literature: most vulnerable groups	Our study
Context: Type	Spear (instead of ‘general’)	Spear=50% more effective
Sex	3 studies No effect 4 studies: Females but not after training, in 1 study	No effect
Age:	Younger persons	Non-linear relationship, interaction with YoS
Years of service (YoS)	Less YoS	Less YoS But more so with general email
Power distance (measured by country of origin)*	High PDI (much hierarchy)	High PDI (much hierarchy)

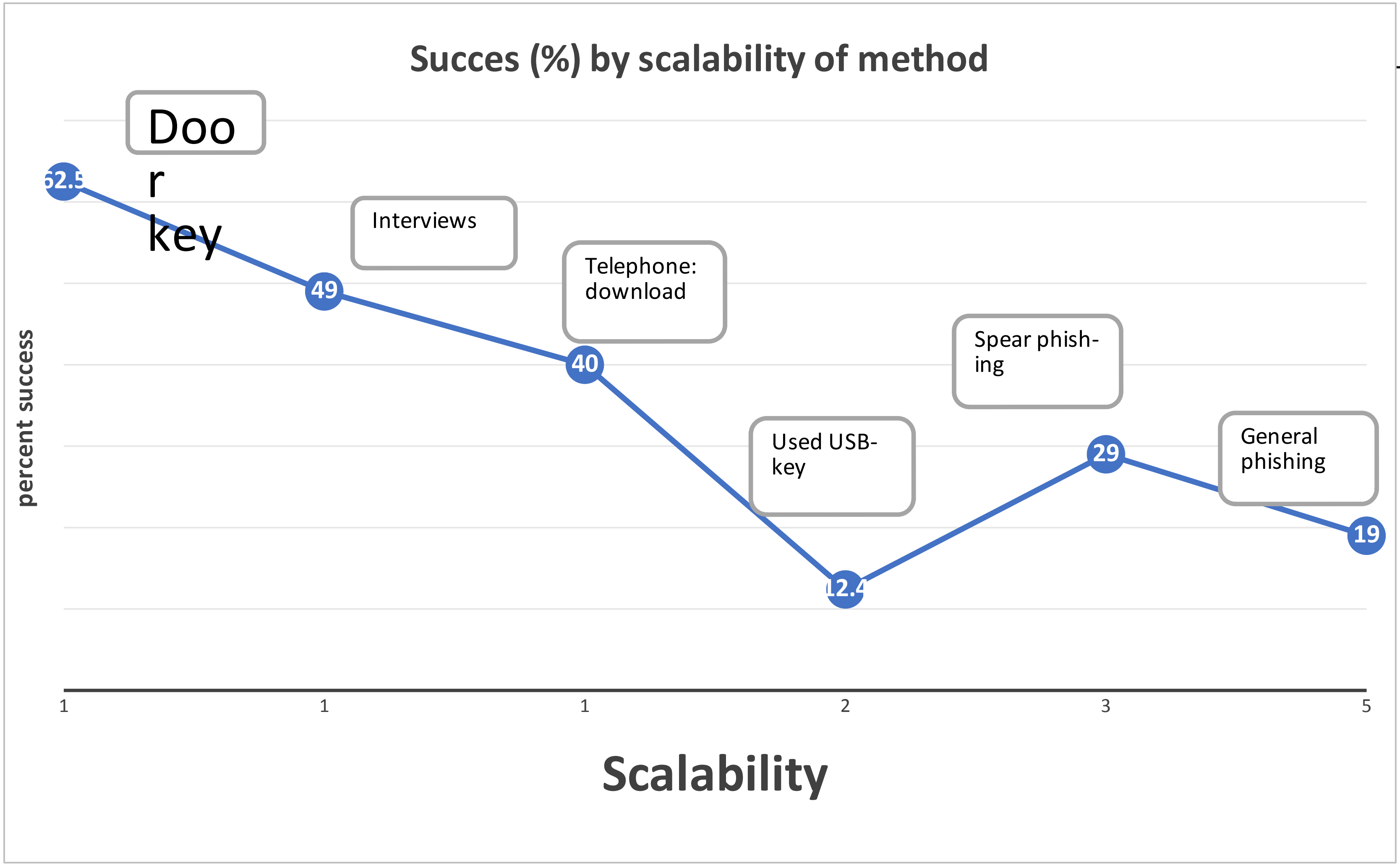
* “the extent to which the less powerful members of organizations and institutions accept and expect that power is distributed unequally” (Hofstede et al, 2010):

Vulnerability to social engineering

USB-key exper.	USB-key control	Door key	Telephone-> downloaded a file	Questions for shoppers	Phishing	
						
					Spear	General
12.4	41.2	62.5	40	49	29	19
2	3	1	1	1	3	5

Scalable: automation
1-> 5

Success of phishing by Scalability



UNIVERSITY OF TWENTE.

How do they do it: Stajano and Wilson

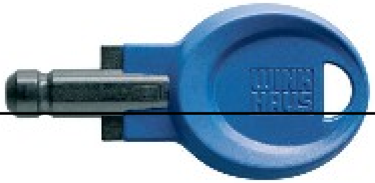
1. Distraction Principle
2. Social Compliance Principle
3. Herd Principle
4. Dishonesty Principle
5. Kindness Principle
6. Need and Greed Principle
7. Time Principle

Stajano, F., & Wilson, P. (2011). Understanding scam victims: seven principles for systems security. Communications of the ACM, 54(3), 70-75.

2. Can we prevent social engineering?

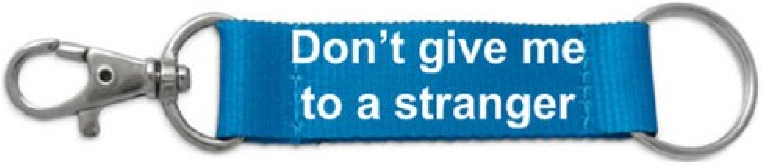
1. Preventive experiments done with
   - **Key experiment**
   - **Telephone-based social-engineering**
   - **Questions for shoppers: ‘Can I get your bank account number?’**
   - Spear versus ‘traditional’ phishing emails
   - Phishing prevention experiment with children

Door-key experiment



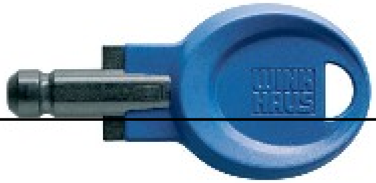
Intervention:

1. a leaflet explaining social engineering
2. a blue key chain
3. a poster with
   - A humorous quote
   - An explicit remark against password, key and PIN sharing



Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. Journal of Experimental Criminology,

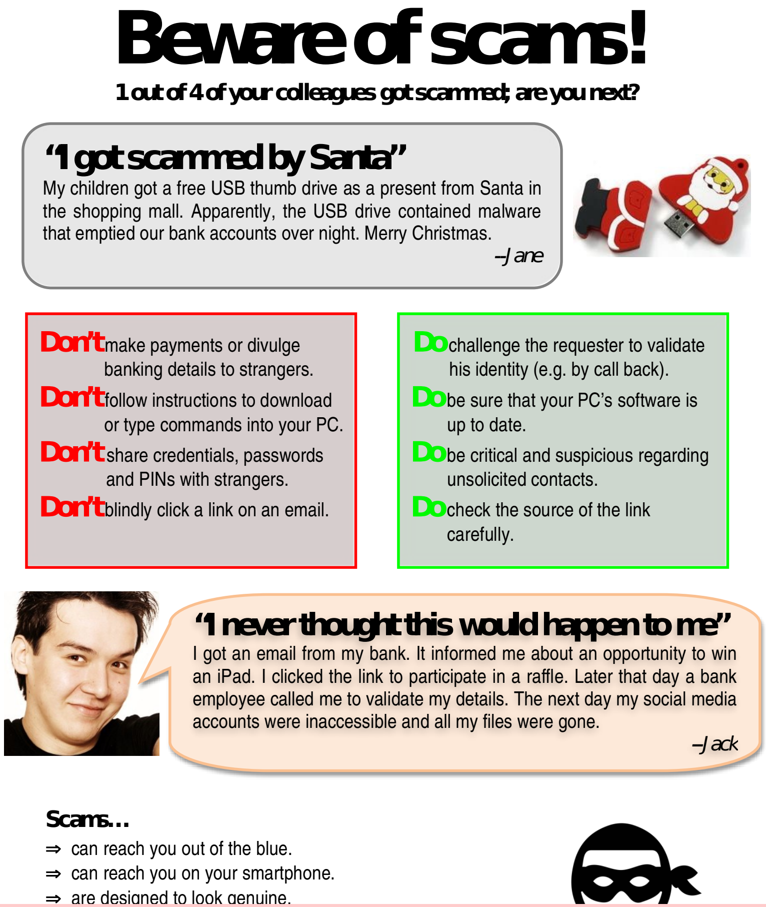
Door key experiment



	No intervention	Intervention
Complied – handed over the key, in %	**62.5**	**37.0**

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. Journal of Experimental Criminology,

Telephone phishing



Beware of scams!

1 out of 4 of your colleagues got scammed; are you next?

"I got scammed by Santa"

My children got a free USB thumb drive as a present from Santa in the shopping mall. Apparently, the USB drive contained malware that emptied our bank accounts over night. Merry Christmas.

–Jane

Don't make payments or divulge banking details to strangers.

Don't follow instructions to download or type commands into your PC.

Don't share credentials, passwords and PINs with strangers.

Don't blindly click a link on an email.

Do challenge the requester to validate his identity (e.g. by call back).

Do be sure that your PC's software is up to date.

Do be critical and suspicious regarding unsolicited contacts.

Do check the source of the link carefully.

"I never thought this would happen to me"

I got an email from my bank. It informed me about an opportunity to win an iPad. I clicked the link to participate in a raffle. Later that day a bank employee called me to validate my details. The next day my social media accounts were inaccessible and all my files were gone.

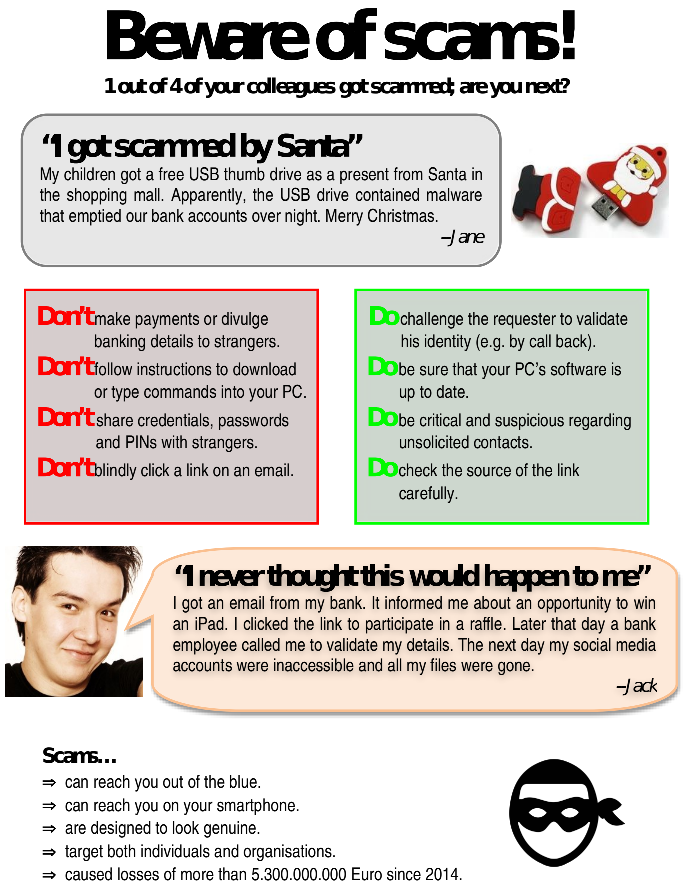
–Jack

Scams…

⇒ can reach you out of the blue.
⇒ can reach you on your smartphone.
⇒ are designed to look genuine.

Bullee, J.-W., Montoya, L., Junger, M., & Hartel, P. (2016, 14-15 Jan 2016). Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention. Paper presented at the Cyber Security R&D Conference (SG-CRC) 2016, Singapore.

Telephone phishing



Beware of scams!

1 out of 4 of your colleagues got scammed; are you next?

"I got scammed by Santa"

My children got a free USB thumb drive as a present from Santa in the shopping mall. Apparently, the USB drive contained malware that emptied our bank accounts over night. Merry Christmas.

–Jane

Don't make payments or divulge banking details to strangers.

Don't follow instructions to download or type commands into your PC.

Don't share credentials, passwords and PINs with strangers.

Don't blindly click a link on an email.

Do challenge the requester to validate his identity (e.g. by call back).

Do be sure that your PC's software is up to date.

Do be critical and suspicious regarding unsolicited contacts.

Do check the source of the link carefully.

"I never thought this would happen to me"

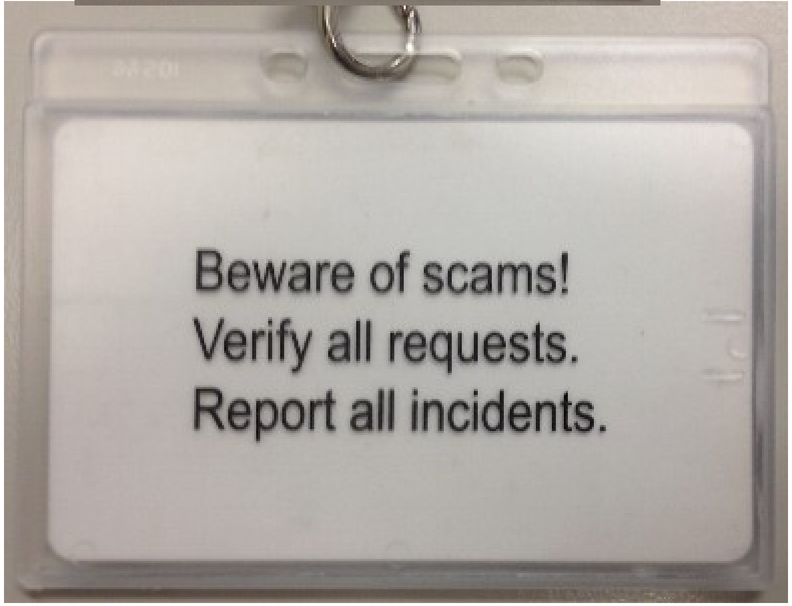
I got an email from my bank. It informed me about an opportunity to win an iPad. I clicked the link to participate in a raffle. Later that day a bank employee called me to validate my details. The next day my social media accounts were inaccessible and all my files were gone.

–Jack

Scams…

⇒ can reach you out of the blue.
⇒ can reach you on your smartphone.
⇒ are designed to look genuine.
⇒ target both individuals and organisations.
⇒ caused losses of more than 5.300.000.000 Euro since 2014.

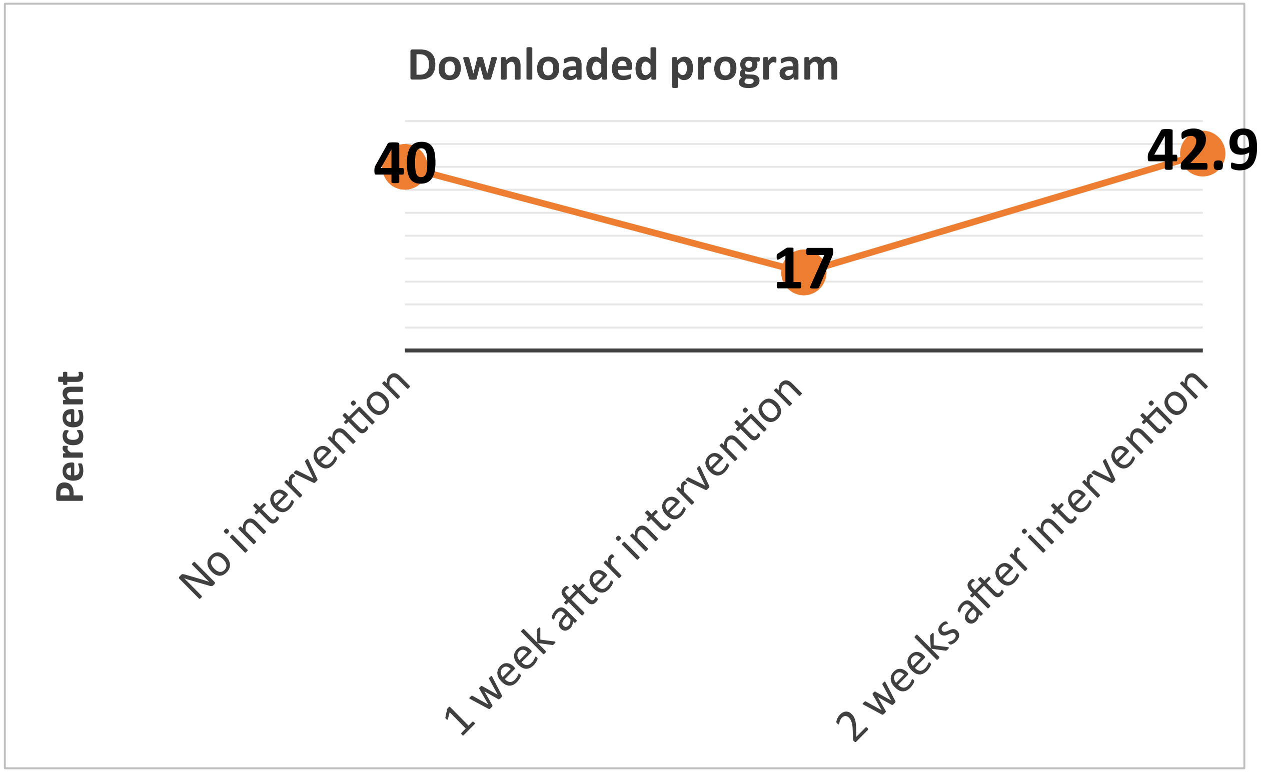
UNIVERSITY OF TWENTE.



Beware of scams!
Verify all requests.
Report all incidents.

Telephone phishing

% Complied: downloaded the program (N=92)

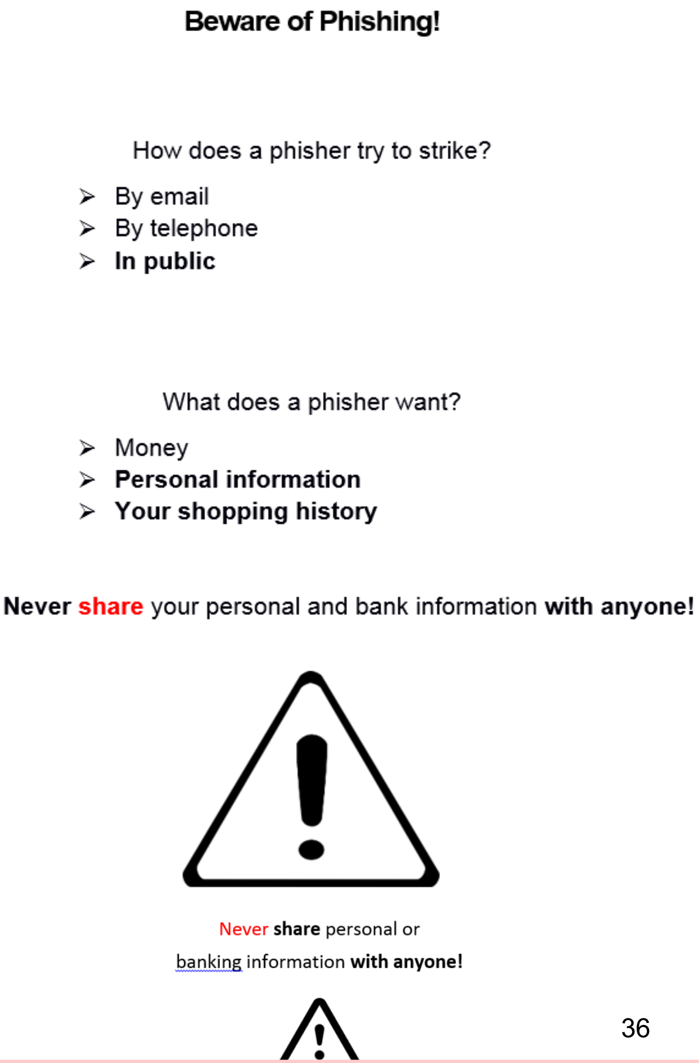


Bullee, J.-W., Montoya, L., Junger, M., & Hartel, P. (2016, 14-15 Jan 2016). Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention. Paper presented at the Cyber

Questions for shoppers: warnings and cues

Priming/cues: ‘Subtle warning’

1. Are you familiar with the term phishing?
2. Are you aware of the amount of personal information you share on the Internet and that is publicly accessible?
3. Do you use Facebook? If so, what are generally your privacy settings?
4. Have you ever been scammed on the Internet (for example through phishing)?



Beware of Phishing!

How does a phisher try to strike?

- By email
- By telephone
- **In public**

What does a phisher want?

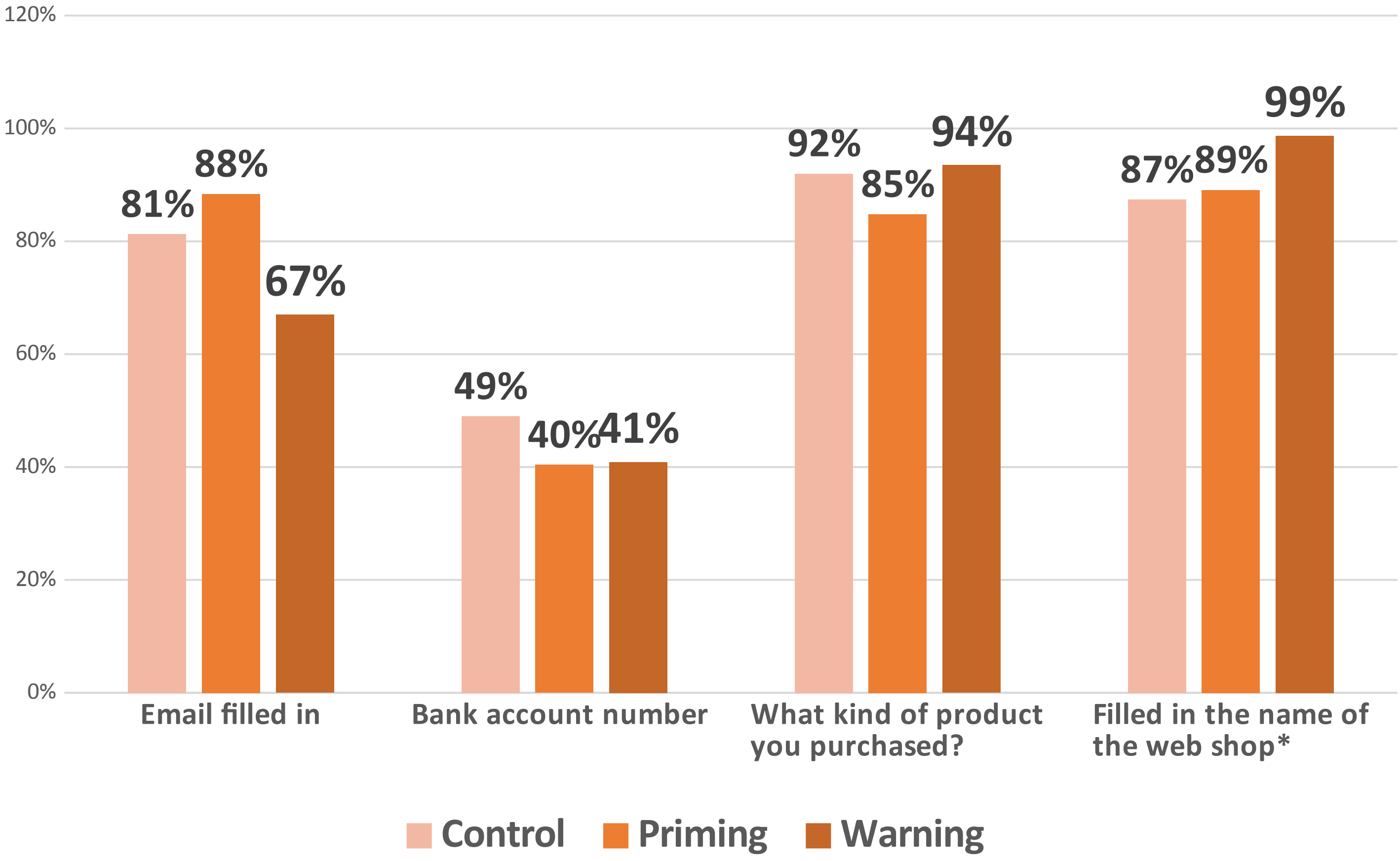
- Money
- **Personal information**
- **Your shopping history**

Never share your personal and bank information **with anyone!**

Never **share** personal or banking information **with anyone!**

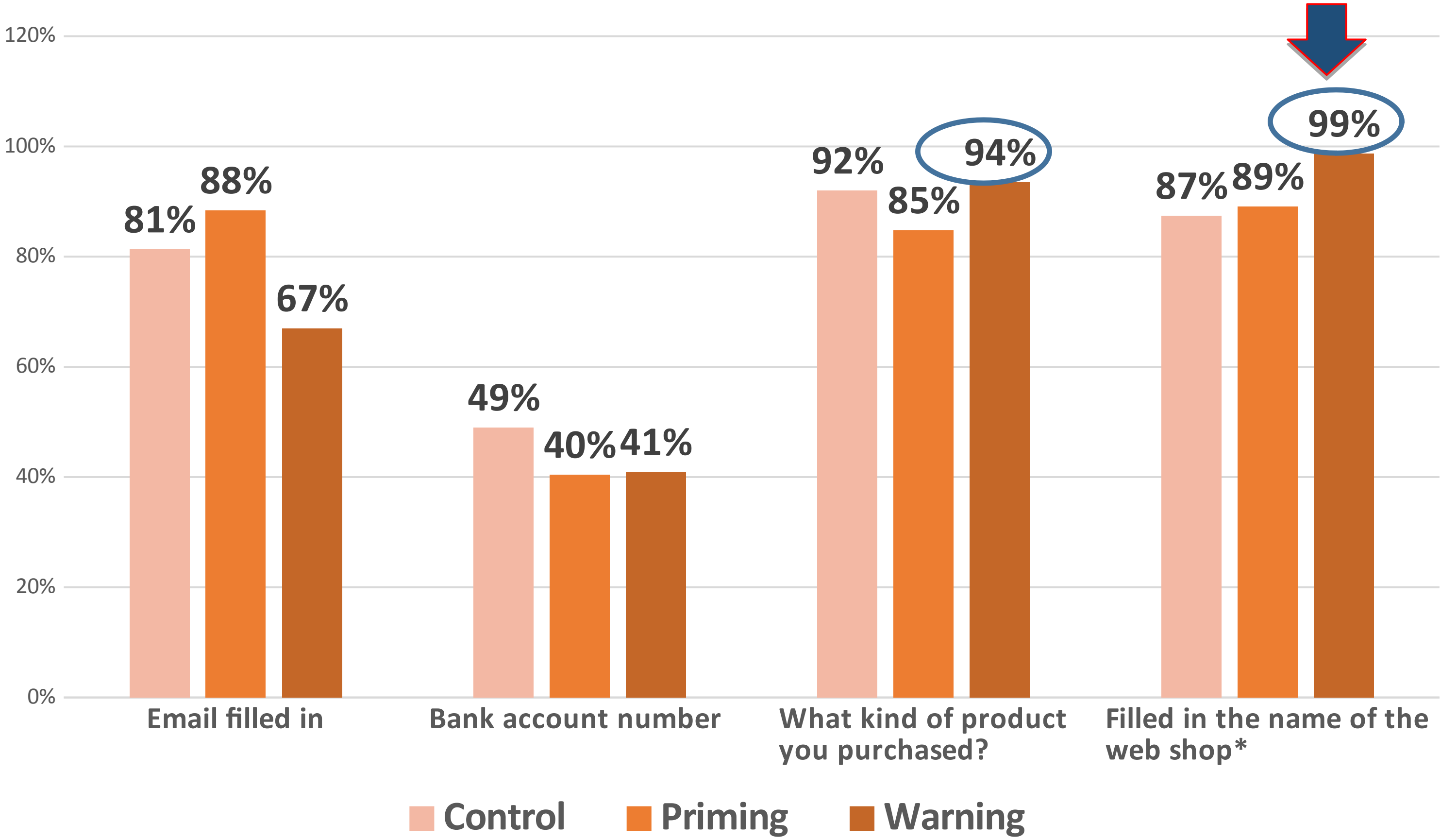
Junger, M., Montoya Morales, A. L., & Overink, F. J. (2017). Priming and warnings are not effective to prevent

Warnings and cues



Junger, M., Montoya Morales, A. L., & Overink, F.-J. (2017). Priming and warnings are not effective to prevent

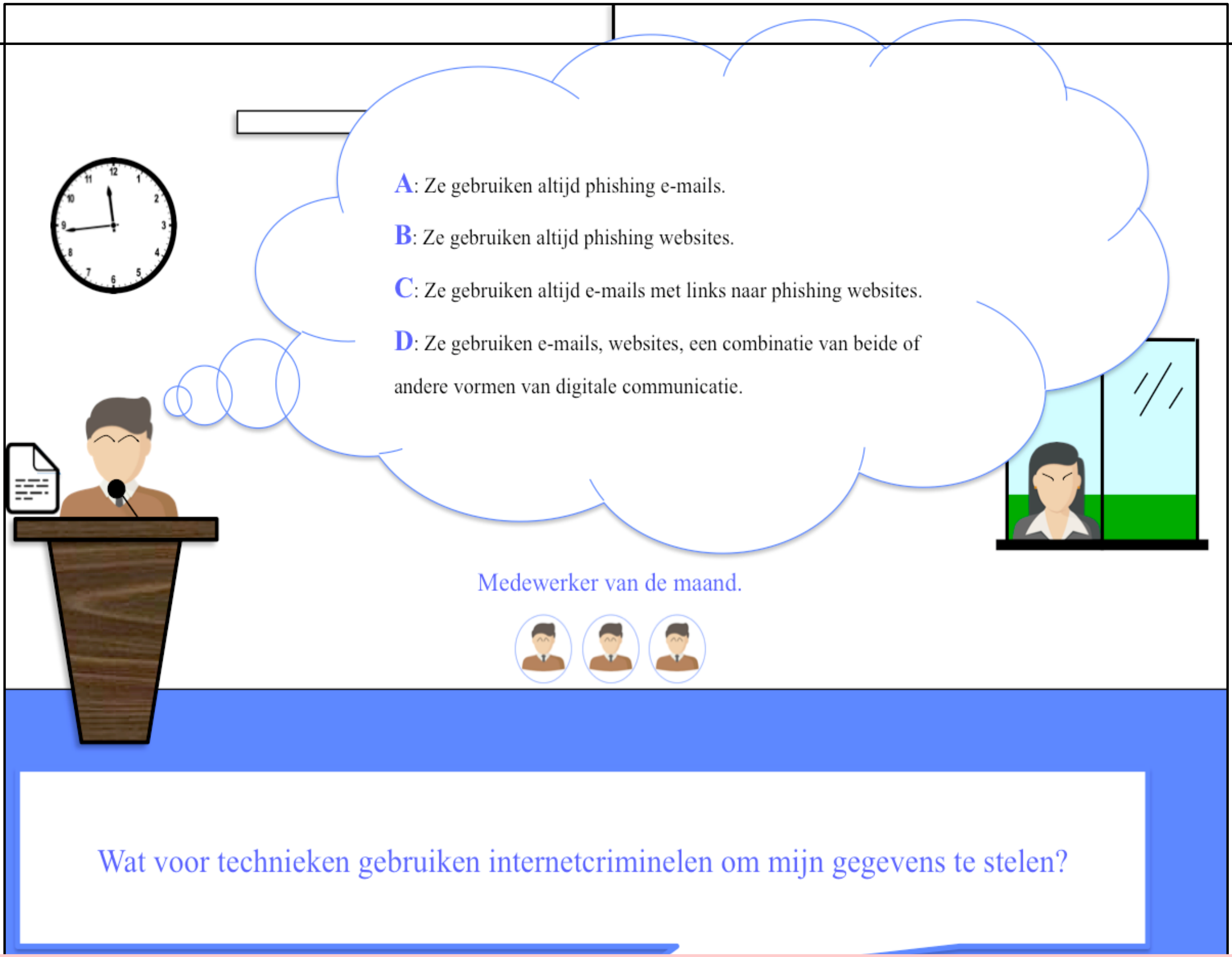
Warnings and cues



Junger, M., Montoya Morales, A. L., & Overink, F.-J. (2017). Priming and warnings are not effective to prevent social engineering attacks. Computers in Human Behavior, 66, 75-87.

Anti-phishing training

Correctly Identified Phishing Emails



A: Ze gebruiken altijd phishing e-mails.

B: Ze gebruiken altijd phishing websites.

C: Ze gebruiken altijd e-mails met links naar phishing websites.

D: Ze gebruiken e-mails, websites, een combinatie van beide of andere vormen van digitale communicatie.

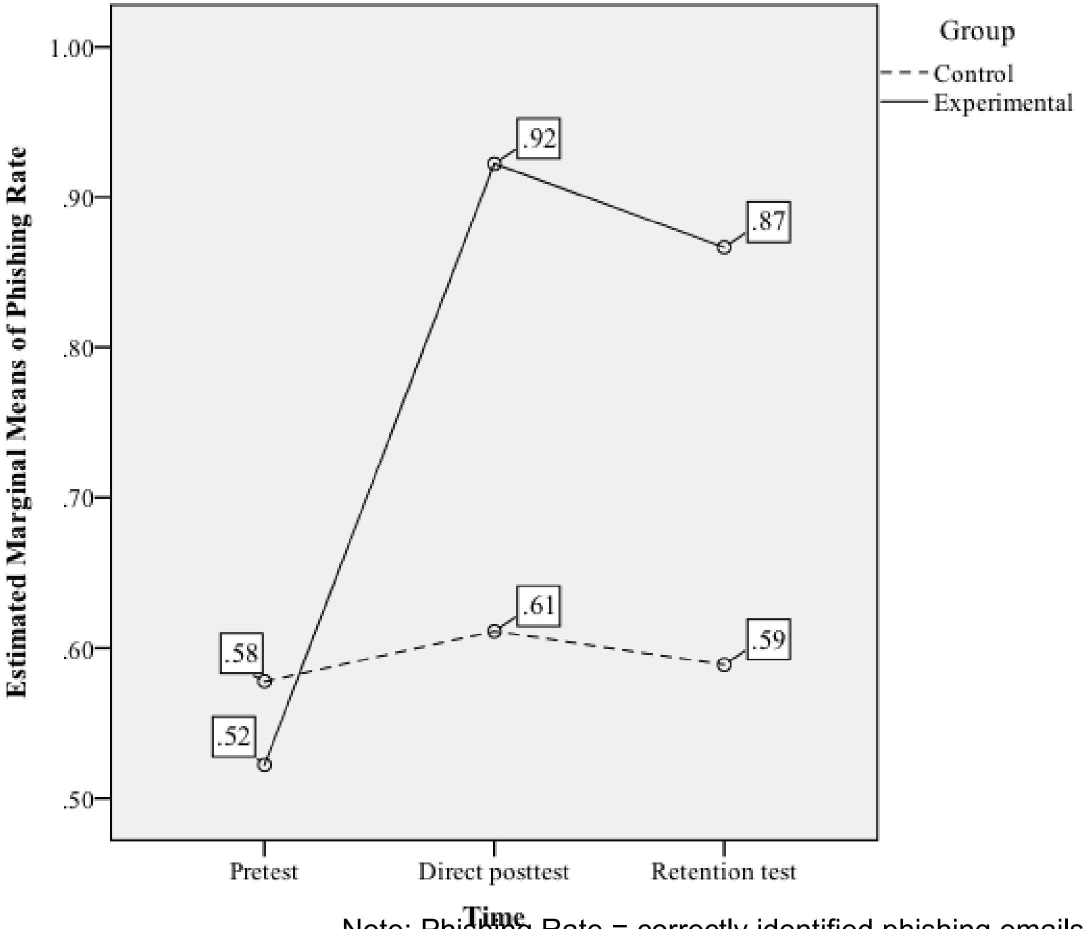
Medewerker van de maand.

Wat voor technieken gebruiken internetcriminelen om mijn gegevens te stelen?

Pars, C. (2017). PHREE of Phish: The Effect of Anti-Phishing Training on the Ability of Users to Identify Phishing Emails. University of Twente, Enschede, Nl.

Anti-phishing training

Correctly Identified Phishing Emails



Note: Phishing Rate = correctly identified phishing emails / number of phishing emails (5)

Pars, C. (2017). *PHREE of Phish: The Effect of Anti-Phishing Training on the Ability of Users to Identify Phishing Emails. University of Twente, Enschede, Nl.*

Conclusions: Gullibility

1. Humans are programmed to trust
    - Op to 80% is ‘engineered’
    - Truth bias

2. Interventions seem easy as well: counter-manipulation

Gullibility: Development of trust: infants

1. ‘A human child is shaped by evolution to soak up the culture of her people’, Dawkins 1993
   - Dawkins, R. (1993). Viruses of the mind. Dennett and his critics: Demystifying mind, 13-27, p. 13
   - Morgan TJH and Laland KN. (2012) The Biological Bases of Conformity. Frontiers in Neuroscience 6: 87.
   - Harris PL, Corriveau K, Pasquini ES, et al. (2012) Credulity and the development of selective trust in early childhood. In: Beran MJ, Brandl J, Perner J, et al. (eds) Foundations of Metacognition. Oxford, UK: Oxford University Press, 193.
   - Harris PL and Corriveau KH. (2011) Young children's selective trust in informants. Philosophical Transactions of the Royal Society B: Biological Sciences 366: 1179-1187.
   - Koenig MA and Harris PL. (2007) The Basis of Epistemic Trust: Reliable Testimony or Reliable Sources? Episteme 4: 264-284.

2. Deception research: Truth-bias.
   - Burgoon JK and Buller DB. (2015) Interpersonal Deception Theory. In: Gass RH and Seiter JS (eds) Readings in Persuasion, Social Influence, and Compliance Gaining. Boston, MA: Allyn & Bacon.
   - Burgoon JK and Levine TR. (2010) Advances in deception detection. New directions in interpersonal communication research: 201-220.

Conclusions: Gullibility

1. Relatively stable characteristic of humans
    - Don’t blame the victims!

2. Good protection is hard

3. Humans forget easily

* Fransen, M. L., Smit, E. G., & Verlegh, P. W. (2015). Strategies and motives for resistance to persuasion: an integrative framework. Frontiers in psychology, 6.
** Stajano, F., & Wilson, P. (2009). Understanding scam victims: seven principles for systems security (754). Retrieved from University of Cambridge, Computer Laboratory: Available at: http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-754.pdf

Why are interventions difficult? Processes at work

1. Social proof (observing others)

2. Lack of knowledge: no link intervention between PII - attack

3. Optimism bias

4. Personal relevance – when one was victimized

5. ‘Who’ is more important than ‘what’

* Fransen, M. L., Smit, E. G., & Verlegh, P. W. (2015). Strategies and motives for resistance to persuasion: an integrative framework. Frontiers in psychology, 6.
** Stajano, F., & Wilson, P. (2009). Understanding scam victims: seven principles for systems security (754). Retrieved from University of Cambridge, Computer Laboratory: Available at: http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-754.pdf

Adverse effects – also in security

1. Known in physical world ‘some interventions have adverse effects (Fransen, Smit, & Verlegh, 2015; Fransen, Verlegh, Kirmani, & Smit, 2015).

2. Review of ‘perverse effects’ in digital world (Wolff, 2016)

3. Resistance to ‘manipulation’:
   - Avoidance - cognitive avoidance
   - Optimism bias, no personal relevance
   - Difficult passwords

- Weinstein, N. D., & Klein, W. M. (1995). Resistance of personal risk perceptions to debiasing interventions. *Health Psychology, 14(2), 132.*
- Fransen, M. L., Smit, E. G., & Verlegh, P. W. J. (2015). Strategies and motives for resistance to persuasion: an integrative framework. *Frontiers in psychology, 6*
- Fransen, M. L., Verlegh, P. W. J., Kirmani, A., & Smit, E. G. (2015). A typology of consumer strategies for resisting advertising, and a review of mechanisms for countering them. *International Journal of Advertising, 34*(1), 6-16. doi:10.1080/02650487.2014.995284Wolff, J. (2016). *Perverse Effects in Defense of Compute Systems: When More Is Less. Paper presented at the 2016 49th Hawaii International Conference on System Sciences, Hawaii, US.*

UT studies

1. Bullee, J.-W. (2017). Experimental social engineering: investigation and prevention. (PhD), University of Twente, Enschede.
2. Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. Journal of Experimental Criminology, 11(1), 97-115. doi: 10.1007/s11292-014-9222-7
3. Bullee, J.-W., Montoya, L., Junger, M., & Hartel, P. (2016, 14-15 Jan 2016). *Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention. Paper presented at the Cyber Security R&D Conference (SG-CRC) 2016, Singapore.*
4. Bullee, J.-W., Montoya, L., Junger, M., & Hartel, P. (2017). Spear phishing in organisations explained. *Information and Computer Security. doi: https://doi.org/10.1108/ICS-03-2017-0009*
5. Junger, M., Montoya Morales, A. L., & Overink, F.-J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior, 66, 75-87.*
6. Lastdrager, E., Montoya, L., Hartel, P., & Junger, M. (2013). Applying the Lost-Letter Technique to Assess IT Risk Behaviour Proceedings of the 3rd Workshop on Socio-Technical Aspects in Security and Trust. 29 Jun 2013, New Orleans, USA. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6691363&queryText%3Dmontoya%2C+lastdrager (pp. 2-9): IEEE Computer Society.
7. Lastdrager, E., Montoya, L., Hartel, P., & Junger, M. (2013). Preventing phishing with children (forthcoming)
8. Montoya, L., Junger, M., & Hartel, P. (2013). How 'Digital' is Traditional Crime? European Intelligence and Security Informatics Conference (EISIC) 2013, 31-37. Retrieved from: http://ieeexplore.ieee.org/search/searchresult.jsp?newsearch=true&queryText=how+digital+is+traditional+crime%2C+montoya&x=-1280&y=-331
9. Pars, C. (2017). *PHREE of Phish: The Effect of Anti-Phishing Training on the Ability of Users to Identify Phishing Emails. University of Twente, Enschede, Nl.*

QUESTIONS?

Thank you!

You can also mail me: m.Junger@utwente.nl

How to improve security in organizations (1) Interventions

New methods need to be found and experimented with:

1. Blame-free reporting
2. Exercises & training
    - Mock attacks – in combination with training and testing
3. Individual versus group approach
4. Focus of specific groups (new employees)

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society, 32(3), 183-196. doi: 10.1016/j.techsoc.2010.07.001*

Caldwell, T. (2013). Spear-phishing: how to spot and mitigate the menace. *Computer Fraud & Security, 2013(1), 11-16. doi: http://dx.doi.org/10.1016/S1361-3723(13)70007-1*

Sasse, M. A., Ashenden, D., Lawrence, D., Coles-Kemp, L., Fléchais, I., & Kearney, P. (2007). Human vulnerabilities in security

How to improve security in organizations
(2) Policies

New methods need to be found and experimented with:

1. Secure Messaging Portals for communication *within* the organization
2. Put security on the agenda in periodic meetings.
   - Inform on - and discuss incidents
   - Discuss security policies and counter measures

Bullee, J.-W. (2017). Experimental social engineering: investigation and prevention. (PhD), University of Twente, Enschede.

How to improve security in organizations (3)

1. Experimenting more systematically to learn more on
   - the general principles
   - the specific points for organizations
2. Aim at more accumulation of knowledge *(next slides)*

How to improve security in organizations (4) Share knowledge in a common database

1. Analysis of incidents (no exclusive focus on vulnerabilities)
2. Share data on incidents with others
3. Share data on penetration tests with others
4. Include data on departments and individual characteristics
5. Set up common database (anonymized)
   - with information on incidents, and data from experiments

QUESTIONS?

Thank you!

You can also mail me: m.Junger@utwente.nl

UT studies

1. Bullee, J.-W. (2017). Experimental social engineering: investigation and prevention. (PhD), University of Twente, Enschede.
2. Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. Journal of Experimental Criminology, 11(1), 97-115. doi: 10.1007/s11292-014-9222-7
3. Bullee, J.-W., Montoya, L., Junger, M., & Hartel, P. (2016, 14-15 Jan 2016). *Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention. Paper presented at the Cyber Security R&D Conference (SG-CRC) 2016, Singapore.*
4. Bullee, J.-W., Montoya, L., Junger, M., & Hartel, P. (2017). Spear phishing in organisations explained. *Information and Computer Security. doi: https://doi.org/10.1108/ICS-03-2017-0009*
5. Junger, M., Montoya Morales, A. L., & Overink, F.-J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior, 66, 75-87.*
6. Lastdrager, E., Montoya, L., Hartel, P., & Junger, M. (2013). Applying the Lost-Letter Technique to Assess IT Risk Behaviour Proceedings of the 3rd Workshop on Socio-Technical Aspects in Security and Trust. 29 Jun 2013, New Orleans, USA. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6691363&queryText%3Dmontoya%2C+lastdrager (pp. 2-9): IEEE Computer Society.
7. Lastdrager, E., Montoya, L., Hartel, P., & Junger, M. (2013). Preventing phishing with children (forthcoming)
8. Montoya, L., Junger, M., & Hartel, P. (2013). How ‘Digital’ is Traditional Crime? European Intelligence and Security Informatics Conference (EISIC) 2013, 31-37. Retrieved from: http://ieeexplore.ieee.org/search/searchresult.jsp?newsearch=true&queryText=how+digital+is+traditional+crime%2C+montoya&x=-1280&y=-331
9. Pars, C. (2017). *PHREE of Phish: The Effect of Anti-Phishing Training on the Ability of Users to Identify Phishing Emails. University of Twente, Enschede, Nl.*