Social Engineering & Cyber Security

Marianne Junger
University of Twente

M.Junger@Utwente.nl
http://www.utwente.nl/bms/iebis/staff/junger
Colleagues

Pieter Hartel
Elmer Lastdrager
Lorena Montoya
Jan-Willem Bullee
Wolter Pieters
Aim: Prevention experiments and what we learned

1. Door key experiment
2. Telephone-based social-engineering
3. Can I get your bank account number?
EXP 1. Door Key Experiment: Can I have your key, please?

- 118 rooms
- Story ‘recharge key’
- Compliance: 62.5%

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
## Door-Key Experiment

<table>
<thead>
<tr>
<th></th>
<th>No intervention</th>
<th>Intervention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complied</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(versus handed over the key)</td>
<td>62.5 %</td>
<td>37.0 %</td>
</tr>
</tbody>
</table>
EXP 2. Telephone phishing

Frequently used method to contact consumers (29.9% of all scams)

• ‘attackers’ targeted in total 45 UT-staff

• Story:
  – “your PC is sending spam,
  – You can download a program that will remove the malware”

• Subgroup: N (control group)=26 -> 46.2% downloaded the program


National Consumer League
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.
**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.
% Complied: downloaded the program

- 46.2% for No intervention
- 9.1% for 1 week intervention
- 54.6% for 2 weeks intervention
EXP 3. Street questionnaires

- 278 questionnaires filled in in shopping area
- 3 page questionnaire on cyber security
- How easy is it to collect information for spear phishing?
  1. Can you fill in your email address?
  2. Bank account: ☐☐ XX ☐☐☐☐ Xxxxxxx ☐☐☐
     Online shoppers only
  3. What kind of product you purchased?
  4. Filled in the name of the web shop

Junger, M., Montoya, L., & Overink, F.-J. (Under review). Warnings and cues against social engineering.
Street questionnaire: 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)?
Priming and warning: not effective

- Email filled in **
- Bank account number
- What kind of product you purchased?
- Filled in the name of the web shop*

Control  Priming  Warning

Percent

81%  81%
88%  85%
67%  94%
49%  92%
41%  94%
40%  99%
67%  87%
41%  89%
40%  87%
## Warnings: adverse effect

<table>
<thead>
<tr>
<th>Email filled in **</th>
<th>Bank account number</th>
<th>What kind of product you purchased?</th>
<th>Filled in the name of the web shop*</th>
</tr>
</thead>
<tbody>
<tr>
<td>88%</td>
<td>67%</td>
<td>49%</td>
<td>85%</td>
</tr>
<tr>
<td>81%</td>
<td>41%</td>
<td>40%</td>
<td>87%</td>
</tr>
<tr>
<td>92%</td>
<td>94%</td>
<td>99%</td>
<td>89%</td>
</tr>
<tr>
<td>99%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Conclusions: trust

• Humans are programmed to trust: social engineering is easy
  – 10%-90% is ‘engineered’

• Interventions seem easy as well: counter-manipulation
Why did some interventions not work?

- No intervention
- Social proof (observing others)
- Lack of knowledge – no link intervention – PII that was given
- Optimism bias
- Personal relevance – when one was victimized
Adverse effect – also in security

• Know in physical world ‘When confronted with risks, people can use self-serving strategies to justify their unrealistic optimism (Weinstein & Klein, 1995).

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

• Resistance to ‘manipulation’:
  – Avoidance - cognitive avoidance
  – Optimism bias, no personal relevance


How to improve our interventions?

- Increase personal relevance - CMU interventions only for those who have been phished
- Training: better-stronger trainings
- Repeated interventions – not one training but a process

Question: can we really protect users against phishing?
Questions?

M.Junger@Utwente.nl

http://www.utwente.nl/bms/iebis/staff/junger/
Questions?

M.Junger@Utwente.nl

http://www.utwente.nl/bms/iebis/staff/junger/