DEPARTMENT OF COMPUTER SCIENCE

UNIVERSITY OF OXFORD

Informal Support Networks: an investigation into Home Data Security Practices

Norbert Nthala

Ivan Flechais

Why Study the Home?

- Internet use in homes is high, networked devices are proliferating
  - 74.4 percent of all [U.S.] households in 2013[1]
  - 86 percent (22.5 million) of households in Great Britain in 2015[2]
- Personal and home use of (work and non-work) services is growing
- Increased threats and attacks *to* and *from* the home
  - "Home users were the most highly targeted sector, accounting for 95 percent of all targeted attacks" – Symantec Internet Security Threat Report 2007 [3]
  - DDoS from compromised home devices (e.g. Lizard Squad Christmas 2014 DDoS against Xbox Live and PlayStation Network allegedly used 250K – 500K infected home routers; Dyn DNS hack of October 2016)
- Unlike (most) organisations, homes have no explicit support dedicated to mitigating threats, keeping up-to-date, and procuring and managing controls

[1] U.S. Department of Commerce, Economics and Statistics Administration. Computer and internet use in the United States: 2013
[2] Office for National Statistics. Internet access - households and individuals 2015. http://www.ons.gov.uk/ons/dcp171778_-412758.pdf.
[3] Symantec Internet Security Threat Report, Trends for January–June 07: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf

State of the Art in Home Data Security

- *AWARENESS* [1, 2, 3, 4, 5]
- Security behaviours
  - Antivirus, patching, data backup, parental controls
- Success?
  - Not much [1, 6, 7, 8]

[1] Improving protection and security awareness among home users
[2] So long, and no thanks for the externalities: the rational rejection of security advice by users
[3] Teaching Johnny not to fall for phish
[4] Social information leakage: Effects of awareness and peer pressure on user behavior
[5] I think they're trying to tell me something: Advice sources and selection for digital security
[6] Computer security and risky computing practices: A rational choice perspective
[7] Assessing the security perceptions of personal internet users
[8] Hey, I have a problem in the system: Who can help me? an investigation of Facebook users interaction when facing privacy problems

State of the Art in Home Data Security

- What Next?
  - Explore alternatives to increasing awareness
- Interdisciplinary approaches proposed
  - [9,10,11,12]

[9] Pools, clubs, and security: designing for a party not a person.
[10] Applying problem-structuring methods to problems in computer security.
[11] Influencing mental models of security: a research agenda.
[12] Towards the realization of a public health system for shared secure cyber-space

Research Questions

- What influences security decision-making in the home?
- Where do home users get support?
- What are the characteristics of security support in the home?

Research Methods

- Phase 1: Qualitative exploration of the problem domain
  - 15 semi-structured scoping interviews
  - Data collection: *50 semi-structured interviews* with home users in the UK
  - Data analysis: *Grounded Theory*
- Phase 2: Quantitative study to validate and generalise qualitative findings
  - Platforms used: *Unipark* and *Prolific Academic*
  - Number of participants: *1128 UK residents*
  - Data analysis: *Descriptive and inferential statistics*
    - Frequency tables, bar charts
    - Tests for ranking, association, difference

What we found

- Factors influencing security decision-making
  1. Survival/Outcome bias
  2. Other factors related to one's confidence in a security measure
  3. Availability and quality of security support
- Evaluating available and quality of support
  - Perceived competence, trust, cost, closeness, availability
- Preference in source of security support
  - Relative, Friend, Work colleague, IT repair shop professional, service provider/manufacturer help desk, others
- Characteristics of security support
  - Duty of care
  - Continuity of care

Survival/Outcome bias

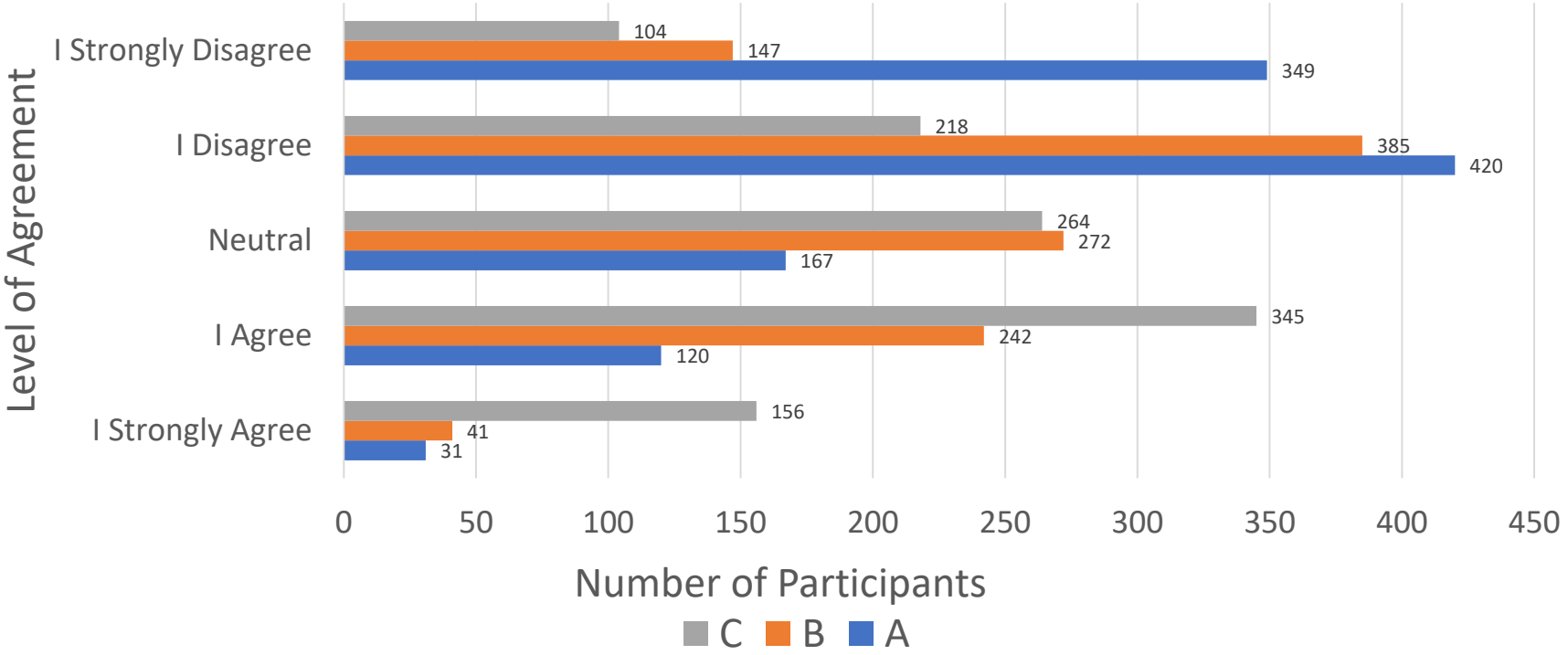
"I think it's probably the fact that as far as I'm aware of, I haven't had serious breaches of personal data, or data security breaches. Not that I'm aware of, no. I think if I was exposed to something which was quite serious, then I would probably change my look quite a lot" – P6

For the past 5 years, your friend John has been downloading free music, videos, and software from different websites including torrent sites without any problem. One day, he reads an article about the dangers of free downloads such as viruses, adware, Trojan horses, worms and spyware. For each of the following options, how much do you agree that it is a good choice for John?

A - *Continue downloading free les from any website as usual. He has been doing it for 5 years without a problem, chances of being affected are very small.* **(~ 22% ✔)**

B - *Restrict the downloads to those websites John has already used before. He has used them for 5 years without a problem, he trusts them to be secure.* **(~ 44% ✔)**

Other factors that induce or undermine confidence



- A – Take no action (*control variable*).
- B – Rely on an antivirus.
- C – Rely on data backup.

- Wilcoxon signed-rank test:
  - A vs B (*Z* = -16.473, *p* = 0.000)
  - A vs C (*Z* = -14.497, *p* = 0.000)

Evaluating available & quality of support

1. Perceived competence (**91%**)
2. Trust (**89 %**)
3. Availability (**31 %**)
3. Cost to one seeking support (**49%**)
4. Closeness (**31%**)
5. Cost to the source of support (**36%**)

- *Ranking*
  - *Friedman test ($X^2(5) = 2444.265, p < .05$)*
  - *Post hoc analysis with Wilcoxon signed-rank test*
  - *With Bonferroni correction applied: p = 0.003*

Assessing Perceived Competence

- How do home users assess someone's security competence?
  1. He/she works in data security (**86%**)
  2. He/she studied or studies data security (**78%**)
  3. He/she has more experience than you in using or working with technical devices and services (**51%**)
  4. His/her job is technical (**24%**)
  5. He/she works for a technical company (**24%**)
  5. He/she studied or studies a technical course (**27%**)

  5. He/she has experienced a data security incident before (**39%**)
  6. He/she is more educated than you (**7%**)
  7. None of the above (**4%**)

- *Ranking*
  - *Friedman test ($X^2(7) = 3218.784, p < .05$)*
  - *Post hoc analysis with Wilcoxon signed-rank test*
  - *With Bonferroni correction applied: $p = 0.002$*

Preference in Seeking & Giving Support

Likelihood of seeking support from:

1. Relative (**80%**) and Friend (**85%**)
2. Service provider/Manufacturer help desk (**58%**)
3. Work colleague (**71%**)
4. IT repair shop professional (**51%**)
5. Others (**16%**)

($X^2(5) = 2066.482$, $p < .05$)…. $P = 0.003$

Give unsolicited support to:

1. Relative (**56%**)
2. Friend (**47%**)
3. Work colleague (**27%**)
4. Others (**12%**)

($X^2(3) = 2127.517$, $p < .05$)…. $P = 0.008$

Accept unsolicited support from:

1. Relative (**63%**) and Friend (**63%**)
2. Work colleague (**48%**) and Service Provider/Manufacturer help desk (**44%**)
3. IT repair shop professional (**40%**)
4. Others (**12%**)

($X^2(5) = 1987.664$, $p < .05$)…. $P = 0.003$

Characteristics of Support: Duty of Care

- Security support is a moral obligation to ensure the well-being of others in society… in 3 ways:

1. Delegation

   …to more competent and trusted others

2. Motivation

   …e.g. by offering unsolicited support

3. Social responsibility

   "…[I give advice] to help her… [and to] everyone if I know them and I am sympathetic to them." – P36.

Characteristics of Support: Continuity of Care

- Home users look for a continuous and caring relationship with the source of support.
  - Helpers are more likely to take responsibility of consequences from any support they offer.

Test Statistics[a]

	A2 - A1	B2 - B1	C2 - C1	D2 - D1	E2 - E1	F2 - F1	G2 - G1	H2 - H1
Z	-.994[b]	-3.035[b]	-4.136[b]	-4.099[c]	-1.262[b]	-15.572[b]	-16.103[b]	-11.571[c]
Asymp. Sig. (2-tailed)	.320	.002	.000	.000	.207	.000	.000	.000

a. Wilcoxon Signed Ranks Test

b. Based on positive ranks.

c. Based on negative ranks.

Conclusions

1. Leverage existing social relationships
   - Build competence, targeting tools, and fostering a sense of trust and recognition
2. Practice evidence-based security
   - Detect and communicate (in a simple, concise, and understandable manner) any attempted, successful, and failed attacks

Thank you!

- Any questions?

References

[1] B. P., F. S.M., and P. A.D. Improving protection and security awareness among home users. *Advances in Networks, Computing and Communications 4*, 2008.

[2] C. Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. *In Proceedings of the 2009 workshop on New security paradigms workshop*, pages 133-144. ACM, 2009.

[3] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong. Teaching johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, 10(2):7, 2010.

[4] M. Nouh, A. Almaatouq, A. Alabdulkareem, V. K. Singh, E. Shmueli, M. Alsaleh, A. Alari, A. Alfaris, et al. Social information leakage: Eects of awareness and peer pressure on user behavior. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 352-360. Springer, 2014.

[5] E. M. Redmiles, A. R. Malone, and M. L. Mazurek. I think they're trying to tell me something: Advice sources and selection for digital security. In *Security and Privacy (SP), 2016 IEEE Symposium on*, pages 272-288. IEEE, 2016.

[6] K. Aytes and T. Connolly. Computer security and risky computing practices: A rational choice perspective. *Journal of Organizational and End User Computing (JOEUC)*, 16(3):22-40, 2004.

[7] S. Furnell, P. Bryant, and A. D. Phippen. Assessing the security perceptions of personal internet users. *Computers & Security*, 26(5):410{417, 2007.

[8] M. S. Mendes, E. Furtado, G. Militao, and M. F. de Castro. Hey, i have a problem in the system: Who can help me? an investigation of Facebook users interaction when facing privacy problems. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 391-403. Springer, 2015.

[9] Z. Dong, V. Garg, L. J. Camp, and A. Kapadia. Pools, clubs and security: designing for a party not a person. In Proceedings of the 2012 workshop on New security paradigms, pages 77{86. ACM, 2012.

[10] P. Gutmann. Applying problem-structuring methods to problems in computer security. In Proceedings of the 2011 workshop on New security paradigms workshop, pages 37{44. ACM, 2011.

[11] R. Wash and E. Rader. Infuencing mental models of security: a research agenda. In Proceedings of the 2011 workshop on New security paradigms workshop, pages 57{66. ACM, 2011.

[12] J. Rowe, K. Levitt, and M. Hogarth. Towards the realization of a public health system for shared secure cyber-space. In Proceedings of the 2013 workshop on New security paradigms workshop, pages 11{18. ACM, 2013.