Institution: University of Bath

Unit of Assessment: C17 Business and Management Studies

Title of case study: Improving national cybersecurity by increasing understanding of susceptibility to spear phishing and phishing attacks

Period when the underpinning research was undertaken: 2007–2012; 2016–2020

Details of staff conducting the underpinning research from the submitting unit:

Name(s):	Role(s) (e.g. job title):	Period(s) employed by submitting HEI:
Adam Joinson	Professor of Information Systems, previously Reader and Senior Lecturer	June 2007 – August 2012; January 2016 – present
Joanna Hinds	Lecturer, previously Research Associate, Teaching Fellow, Research Officer	April 2012 – present
Emma Williams	Research Fellow	January 2016 – November 2017

Period when the claimed impact occurred: 2016–2020

Is this case study continued from a case study submitted in 2014? No

1. Summary of the impact

Research at the University of Bath has contributed to improvements in national cybersecurity, through insights into the prevention of phishing and spear-phishing attacks. The research has significantly enhanced awareness of when and why people are susceptible to phishing attacks, underpinning changes in the practice of government agencies, including the Centre for the Protection of National Infrastructure and HMRC. The research has supported the development and implementation of the UK Government's "Don't take the bait" campaign and the UK's National Cyber Security Centre guidance (2018) on protection against phishing attacks. The research also underpins CybSafe's training resources, which have been used by over 150,000 employees from a range of different organisations.

2. Underpinning research

Cybercrime, including phishing, is estimated to cost the UK GBP27,000,000,000 every year. According to the UK Government's Cyber Security Breaches Survey (2020), almost half of UK businesses reported a cybersecurity attack or breach in the previous 12 months. A survey by the Department for Digital, Culture, Media & Sport (2020) shows that 46% of businesses and 26% of charities reported having experienced cybersecurity breaches or attacks in the last 12 months, with 86% being phishing attacks. Phishing attacks, malicious attempts to influence people, are continuing to proliferate across the globe, aided by the availability of technology that makes it easy to create communications that appear to come from legitimate sources. To address these pressing problems, Professor Joinson (University of Bath, 2007–2012 and 2016–ongoing) led an interdisciplinary research team of Hinds (University of Bath) and Williams (University of Bath and University of the West of England) to improve understanding of the causes of these cybersecurity breaches and possible defences against them, particularly 'phishing' and 'spear-phishing' (targeted) attacks.

Initial research drew together existing literature to develop a new model of susceptibility to online scams, identifying messaging and contextual effects on individual susceptibility to attempts at malevolent influence (R1). These insights were used to create a model of the relationship

between the electronic message, the context in terms of heuristics, emotions, culture and the organisation, and the individual, in particular their self-control, self-awareness, self-deception, approach to risk, motivation, expertise and trust (R2). Further research studied the impact of competing multiple tasks on people's vigilance in relation to fraudulent electronic communications (R3). The research found that people were more likely to click on impersonated fraudulent messages when under greater cognitive load. With funding from the Centre for the Protection of National Infrastructure (CPNI) (F1) and the Centre for Research and Evidence on Security Threats (CREST) (F2), Joinson, Hinds and Williams conducted a project that studied data from simulated phishing attacks within a large organisation that formed part of the UK's critical national infrastructure (R4). This study of the click-rate of over 60,000 emails identified the critical role of message-related factors in explaining susceptibility; in particular, that exploiting a sense of urgency and invoking authority led to substantially higher click-rates. Analysis of focus groups of employees within another critical national infrastructure organisation (R4, funded by F3) reinforced the importance of message-related factors, as well as the importance of organisational context and employee expectations.

The various analyses suggested that a model from health psychology – protection motivation theory – would provide additional insight in understanding the risks (and protective behaviours) people take in a cybersecurity context, and their willingness to seek additional training or information. Protection motivation theory proposes that people's protective action is a function of their perceived vulnerability to a risk, the severity of its impact, and the cost of the response to protect themselves from it. A measure was developed of people's desire to seek more information about phishing emails based on this theory (R5). Building on this work, from 2017–2020, Professor Joinson led the inter-disciplinary EPSRC project 'Cybersecurity across the Lifespan' (F4) that explored how people's cybersecurity vulnerabilities depended on their understanding of the nature of a threat and their available resources to respond to it, and critically examined how existing awareness campaigns often focused on fear-based messaging rather than coping strategies (R6), and has worked with CPNI and CybSafe to develop a new tool to assess and train for phishing in critical national infrastructure organisations (F5).

3. References to the research

R1 Williams, E. J., Beardmore, A. & Joinson, A. N. (2017) 'Individual differences in susceptibility to online influence: A theoretical review', *Computers in Human Behavior* 72, pp. 412-421. DOI: 10.1016/j.chb.2017.03.002

R2 Joinson, A. N., Paine, C. B., Buchanan, T. & Reips, U-D. (2010) 'Privacy, Trust and Self-Disclosure Online', *Human-Computer Interaction* 25(1), pp. 1–24. DOI: 10.1080/07370020903586662

R3 Williams, E. J., Morgan, P. L., & Joinson, A. N. (2017). 'Press accept to update now: Individual differences in susceptibility to malevolent interruptions', Decision Support Systems 96, pp. 119–129. DOI: 10.1016/j.dss.2017.02.014

R4 Williams, E. J., Hinds J. & Joinson, A. N. (2018) 'Exploring susceptibility to phishing in the workplace', International Journal of Human-Computer Studies 120, pp. 1–13. DOI: 10.1016/j.ijhcs.2018.06.004

R5 Williams, E. J., & Joinson, A. N. (2020). 'Developing a measure of information seeking about phishing'. *Journal of Cybersecurity* 6(1). DOI: 10.1093/cybsec/tyaa001

R6 van Steen, T., Norris, E., Atha, K. & Joinson, A. (2020) 'What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use?', *Journal of Cybersecurity* 6 (1). DOI: 10.1093/cybsec/tyaa019

Funders

F1 Individual Differences in Susceptibility to Influence Techniques. Centre for the Protection of National Infrastructure (CPNI). 2016–2018.

F2 CREST - Centre for Research and Evidence on Security Threats (Economic and Social Research Council {ESRC} award: ES/N009614/1). 2016–2020.

F3 Behaviour Change and Security. The National Cyber Security Centre (NCSC). 2017–2018.

F4 CyberSecurity Across the LifeSpan (cSALSA) (Engineering and Physical Sciences Research Council {EPSRC} award: EP/P011454/1). 2016–2020.

F5 Phishtray: Developing a modifiable, open-source email-sorting task for research and training applications related to social engineering. Centre for the Protection of National Infrastructure (CPNI). 2018–2019.

4. Details of the impact

Research at the University of Bath has made a significant impact on national awareness in the prevention of phishing and spear-phishing attacks. The research has contributed to developments in Cabinet Office policy on cybersecurity and improvements in national cybersecurity practice. It has been applied in a range of government and private sector organisations.

Professor Joinson has an established relationship with the Centre for the Protection of National Infrastructure (CPNI) following an 18-month secondment to the UK Government (between 2010 and 2011). This agency (which is part of MI5) is tasked with protecting the UK's national infrastructure from both physical and cyber threats. Joinson is also the Principal Investigator for one of the core programmes of the Centre for Research and Evidence on Security Threats (CREST): 'Understanding and Countering Online Behaviour'. CREST is a national centre whose aim is understanding, mitigating and countering security threats. It is funded by the UK's three security and intelligence agencies (MI5, MI6 and GCHQ), via an ESRC grant (between 2016 and 2020). Joinson has also acted as an academic advisor for the National Cyber Security Centre (NCSC), and is a member of the Behavioural Science Expert Group that advises the National Risk Civil Contingencies Secretariat. The Assistant Director, National Risks Civil Contingencies Secretariat at the Cabinet Office states:

> "*Professor Joinson has challenged assumptions within government and helped us fill gaps in our existing knowledge – thus shaping government policy. Without this expertise, it would be extremely difficult to make robust judgements about risk and our ability to make evidence-based decisions about risk management would be gravely diminished.*
>
> *Professor Joinson's contributions have also shaped the way Local Resilience Forums in England and Wales, as well as the equivalents in Scotland and Northern Ireland, take into account the psychological impacts of emergencies when assessing their local risks. Over 700 specialists from local authorities, police forces, fire and rescue services, ambulance services and utility providers have used the output from Professor Joinson's work to inform local preparations for dealing with emergencies; this figure equates to approximately 50% of all risk specialists in the local responder community*" (S1).

Influencing a national government campaign, "Don't take the bait"

An independent evaluation in 2019 by Lucidity Solutions Ltd noted that "*Joinson's work on phishing has influenced campaign materials and guidance developed by (CPNI) in relation to cybersecurity*" (S2, p. 11). An introductory guide and blog were produced, dealing with the main approaches to phishing and the reasons people click on phishing links (S3). The findings from the research directly influenced the development of campaign materials for the UK government's "Don't take the bait" campaign between 2016 and 2018. These materials incorporated research insights into behavioural influencing factors, such as time pressure and authority, and effective ways of raising awareness of phishing and spear-phishing. The campaign materials included an

animation, introductory and awareness-raising guides, posters, infographic and quiz (S3). The evaluation makes specific reference to the research, stating: "*Joinson's research on spear phishing has been included in a report published by the National Cyber Security Centre on phishing protection and used in guidance prepared by CPNI in relation to phishing simulations*" (S2, p. 4).

Informing national guidance on cybersecurity

Joinson's research has been included in a report on phishing protection (S4), jointly published in 2018 by the CPNI and the NCSC which, as part of GCHQ, acts as a bridge between industry and government. The report was launched at a closed conference organised by NCSC for cybersecurity experts, including approximately 90 chief information security officers of key organisations (e.g. HMRC, BAE, MOD, AWE). In the section of the report entitled 'Carefully consider your approach to phishing training', readers are informed that "*CPNI, in partnership with the University of Bath, have produced a guide (PDF) for what to consider when running phishing simulations*" (S4, p. 9).

Informing the development of training and awareness

Follow-on funding from the CPNI and CREST, and collaboration with CybSafe, led to the development of new training materials and research tools (S2, pp. 4 & 28, S5, S6). Between 2018 and 2019, Joinson and colleagues, working with CybSafe, developed the PHISHTRAY tool and training resources (S2, p. 28). PHISHTRAY is a platform for testing employee susceptibility to phishing emails (S5). It is a modifiable, open-source email-sorting task for research and training applications related to social engineering. It has been used by the Bank of England, BAE, Airbus, HMRC, Babcock and the Home Office (S1, S6).

According to the CEO of CybSafe, the work of Joinson:

> "*… underpins CybSafe technology and our approach to phishing simulations … This has contributed to several hundred organisations gaining insight on what types of phishing attacks and persuasive influences their workforce is susceptible to, allowing them to create more targeted and personalised interventions for their 'high risk' staff. Consequently, over 150,000 people across these organisations have benefited from enhanced anti-phishing behaviour change based on Adam's work*" (S7).

The research has directly impacted on the culture and awareness of cybersecurity at Babcock, which provides engineering services to the defence and civilian sectors and employs over 35,000 people. New approaches to security awareness were implemented using both digital and print materials and an annual 'security conference' (S8). The former Chief Information Security Officer at Babcock stated that: "*It is not an understatement to say that you [Joinson] and your team's contribution to the programme was pivotal in guiding our approach*" (S6).

5. Sources to corroborate the impact

S1 Letter from the Assistant Director, National Risks Civil Contingencies Secretariat of the Cabinet Office, dated 31 July 2019.

S2 Edwards, J. (2019)). *Impact Review: A Review of Impact of the Research Projects Conducted through CREST*. Lucidity Solutions Ltd and The Centre for Research and Evidence on Security Threats. Available at: https://crestresearch.ac.uk/site/assets/files/3427/impact-report-19-028-03.pdf

S3 Compiled set of materials:

- CREST. (2016) *Introductory guide: Why do people click on phishing links*. Available at: https://crestresearch.ac.uk/resources/introductory-guide-phishing/#:~:text=Why%20do%20people%20click%20on%20phishing%20links%3F&text=Phishing%20is%20an%20attempt%20to,links%20or%20filling%20in%20forms.
- CREST & Hinds, J. (2016) *How does phishing work?* Blog. Available at: https://crestresearch.ac.uk/comment/how-does-phishing-work/

- CPNI. *(*2017) *Designing phishing simulations: A quick reference guide for organisations. Don't take the bait.* Available at: https://www.cpni.gov.uk/system/files/documents/51/d7/phishing_simulations_guide.pdf
- CPNI. (2017) *Don't take the bait: Guide for organisations: A personnel security approach to tackling spear phishing*. Available at: https://www.cpni.gov.uk/system/files/documents/18/fe/org%20guide.pdf
- NCSC. (2017) *Multi-layered phishing mitigations.* Campaign material, infographic. Available at: https://www.cpni.gov.uk/system/files/documents/a1/79/Phishing_Attacks_Multi_Layered_Phishing_Mitigations_Infographic.pdf
- NCSC. (2017) *Phishing attacks: Defending your organisation.* Campaign material Available at: https://www.cpni.gov.uk/system/files/documents/63/b4/Phishing_Attacks_Defending_Your_Organisation.pdf
- Phishing and spear phishing (2017). YouTube video. Available at: https://www.youtube.com/watch?v=ygON2B9-xTw
- CPNI. (2017) Posters (phish, bait, trap, smarter, urgency and authority "Are you smarter than a spear phisher?"): Available at:
  Phish https://www.cpni.gov.uk/system/files/documents/cc/d8/phish.pdf
  Bait https://www.cpni.gov.uk/system/files/documents/84/e5/bait.pdf
  Trap https://www.cpni.gov.uk/system/files/documents/08/d3/trap.pdf
  Smarter https://www.cpni.gov.uk/system/files/documents/a4/46/Smarter.pdf
  Urgency https://www.cpni.gov.uk/system/files/documents/f1/39/urgency.pdf
  Authority https://www.cpni.gov.uk/system/files/documents/90/40/authority.pdf
- CPNI. (2017) *Catch the phish*. Infographic. Available at: https://www.cpni.gov.uk/system/files/documents/40/4b/infographic.pdf
- CPNI. (2017) *Catch the phish*. Quiz. Available at: https://www.cpni.gov.uk/system/files/documents/29/97/quiz.pdf

S4 NCSC & CPNI. (2018)). *Phishing attacks: Defending your organisation: How to defend your organisation from email phishing attacks.*

S5 CybSafe. (2020)). *We know what works and what doesn't when it comes to behaviour change.* Available at: https://www.cybsafe.com/about-cybsafe-research-and-analysis/

S6 Testimonial from the Chief Information Security Officer - UK & RoI at BAE Systems plc and former Chief Information Security Officer (2014–2019) at Babcock International Group Plc, dated 6 October 2020.

S7 Testimonial from the CEO of CybSafe, dated 15 October 2020.

S8 Joinson, A. (2019) *Cybersecurity culture guidelines: Behavioural aspects of cybersecurity*. Babcock confidential report. Commissioned by the National Cyber Security Centre (NCSC). Available on request.