The British
Psychological Society
Promoting excellence in psychology

Behaviour Change:
Cybersecurity

Dr John McAlaney, Associate Professor Jacqui Taylor & Helen Thackray
Department of Psychology, Faculty of Science and Technology, Bournemouth University

Recommendations

Cybersecurity is an area that evolves continually and rapidly. Whilst psychological manipulation of cyber-attack victims has been present for many years it is only relatively recently that substantive psychological research in cybersecurity has begun to take place. As such there remains a lack of longitudinal research, and several gaps in the knowledge base. Nevertheless through use of the research that has been conducted and by drawing upon experience in other domains psychology can contribute to addressing challenges encountered in cybersecurity in several ways:

- By using evidence and working with agencies including the National Cyber Security Centre, the British Computer Society and the National Crime Agency to challenge popular stereotypes around hacking that may drive individuals towards criminal activity; and instead highlighting the numerous positive aspects of ethical hacking.
- By working with agencies including the Department of Education to ensure that school curricula covers not only computer programming but also related issues of social responsibility and the risks of engaging in cybercriminal activities.

www.bps.org.uk/behaviourchange

The British
Psychological Society

- By applying behaviour change principles to public and workplace settings to empower individuals to better manage cyber security threats, such as not opening links in phishing emails or disclosing sensitive information that could be used in an attack.
- By contributing expertise and evidence based psychological research knowledge to agencies such as the National Cyber Security Centre who provide advice to employers on the psychological risk factors and behavioural indicators that may suggest employees are either about to unintentionally facilitate a cybersecurity breach or to intentionally instigate one; and how in both instances employees can be supported to reduce these risks.
- By embedding psychological content into the growing number of BSc and MSc cybersecurity courses delivered in the UK.
- By providing guidance to agencies such as Ofcom on the responsible media reporting and depiction of cyber security incidents, to ensure that hacking is not glamourised and that the risks associated with becoming involved in cybercrime are not misrepresented.
- By promoting research into developing a better understanding of why people become involved in hacking, and how they may be encouraged to use their skills and abilities for the protection of cyber systems.

Background

As demonstrated by the number of high profile cases that are regularly reported in the media cybersecurity is a growing societal issue. It impacts on individuals on a personal level, as well as a range of organisations such as governmental bodies, law enforcement agencies and educational institutions. An estimated 6.2 billion cyber-attacks took place globally in 2016 alone[1]. In addition the majority of businesses in the UK state that cybersecurity is either a high or very high priority for them, with 61 per cent of businesses now holding personal data about their customers in an electronic format[2]. As shown in the Wannacry incident of May 2017 and the resulting impact on the NHS cyber-attacks can have real and severe consequences for the general public. Alongside this there is a greater expectation placed upon organisations to secure any data that they retain. The General Data Protection Regulation (GDPR) that came into force (in all EU Member States) in May 2018 specifies that all personal data must be processed in a manner that ensures an appropriate level of security. This includes taking adequate steps to protect against unlawful access to data. A failure to do so can result in substantive penalties being imposed on the organisation.

The cybersecurity threats that society is exposed to are varied. There are financial scams, in which individuals and organisations are tricked into either sending money to a scammer or into installing malicious software, for example, through opening a phishing email. Phishing emails are the single most common attack vector used by cyber adversaries[3], with even the largest technology companies such as Google and Facebook reported to have been the victim of such scams[4]. Other forms of attack include ransomware, in which access to data that an individual or organisation holds is taken from them by an attacker, and effectively held to ransom until a fee is paid. Furthermore, individuals may choose to commit cyber-attacks against nation states due to long standing conflict between nations, which is known as patriotic hacking[5]. Similar to this is hacktivism, in which cyber-attacks are used as a form of social protest, often targeting governments, multi-national companies or other organisations with which they have an ideological clash[6]. Finally cyber-attacks may be committed simply for enjoyment, including the satisfaction of knowing that one has beaten the defences of the target, along with the prestige that may accompany such achievements[7]. In many cases, cyber-attacks involve some form of psychological manipulation, such as, tricking an individual into opening a link within a fraudulent email that results in a virus being installed on their device.

The importance of psychological manipulation in cybersecurity attacks is increasing, since the technological barriers of hacking are decreasing. Software tools for hacking can be obtained online, including on the dark web. This enables those without the necessary technical skills to engage in hacking, who are known within hacking communities as script kiddies. Due to their lack of technical skills such individuals may become involved in criminal activities without a complete understanding of what they are doing, and may in turn put themselves at risk of arrest and prosecution. It has been suggested that the 15 year old boy arrested in relation to the Talk Talk hack of October 2015 was likely a script kiddie[8]. He commented during his trial that his motivation for taking part in the attack had been to impress his friends[9], demonstrating the potential role of social processes in the perpetration of cybersecurity attacks. This increase in cybercrime coincides with an increased emphasis on teaching young people how to write computer code, which is apparent in the number of Coding Clubs that have been created in schools and community centres across the UK. There is a need to ensure that young people with an interest in this area are not only being taught technological skills but also psychological literacy.

The challenge

When considering cybersecurity it is easy to picture media stereotypes of hackers – the hooded figure in a darkened room typing at high speed with computer code flashing across the screen as they breach the defences of their target. However, the same skills that are used by criminal hackers are also used by those who seek to protect systems. The latter includes those known broadly as ethical hackers or ethical security testers, which includes a range of professional titles such as penetration tester. It is important to stress that despite the popular stereotypes 'hacker' in this context does not equate to criminal. Ethical hackers work within the law and are hired by companies and organisations to test their computer systems by attacking them as if they were a criminal hacker with malicious intent. The UK Government is actively working to encourage young people with an interest in cybersecurity to follow this type of career path, through the Cyber Discovery school programme launched in November 2017 (www.joincyberdiscovery.com) and the CyberFirst scheme delivered by the National Cyber Security Centre (www.ncsc.gov.uk/new-talent). These efforts are intended to address the growing skills gap in cybersecurity[10]. Alongside this the National Crime Agency has launched a campaign that seeks to encourage young people to develop their cyber skills for positive outcomes. Making use of the Twitter hashtag #cyberchoices the campaign aims to educate both young people and parents what the consequences may be of becoming involved in cybercrime[11]. It notes that young people who become involved in cybercrime may begin by becoming involved in more trivial activities, such as modifying (modding) video games or launching small scale attacks to temporarily disrupt websites. As they develop their own skills and learn from others these individuals may gradually become involved in more serious criminal activities. The campaign emphasises the benefits of pursuing a legitimate career in cybersecurity, including the very high demand for cybersecurity practitioners, the highly competitive salaries and the opportunities for overseas travel.

One challenge is in acknowledging the innate interest that young people may express in testing and understanding computer systems, whilst steering them away from deviant behaviours and towards the legitimate careers in cybersecurity, where there is high demand. This has parallels to many other behaviour change areas, such as for example prevention and intervention techniques around alcohol use. In the same way that drinking alcohol is not inherently problematic, an interest in hacking and testing the limits of cyber systems is not inherently deviant or criminal. Instead the key point is which pathway people take, and how those at risk of developing a cybercriminal career can be identified, engaged with and encouraged to use their passion and abilities in a positive way in a legitimate cybersecurity career.

The next challenge is to understand the psychological aspects of a cybersecurity incident, so that these can be better mitigated. Whilst cybersecurity is of course a technical area cybersecurity attacks are ultimately composed of a series of behavioural actions, and often include psychological manipulation and deception. The selection of targets by attackers is based, in part, on how vulnerable the attackers perceive the targets to be. The reaction of the targets to being attacked may in turn influence what further actions are taken by the attacker. Whether the target reports the attack may be influenced by concerns about reputation and trust relationships with clients and customers. As has been observed elsewhere, humans remain the weak link in cybersecurity[12]. There is a counter-argument that the one reason cybersecurity attacks are successful is because systems designed to protect organisations fail to take into account psychological characteristics of the individuals who are using these systems. An example would be the requirement for employees to frequently create novel passwords of a certain length and including a combination of letters, numbers and symbols, without perhaps an understanding that a likely outcome of this policy is that people will write these passwords down and leave them close to their computer. To address these issues it is therefore necessary to better understand the psychological factors relevant to this field, and how change may be brought about to better protect society from cybersecurity threats.

What can psychology offer?

Understanding identity and motivation

Cybersecurity attacks would often seem to be a result of group activity, although one of the biggest challenges in cybersecurity is identifying and attributing blame. Those who have claimed responsibility for some of the more high profile cybersecurity incidents chose group names that would suggest they operate as a group, such as Lizard Squad or The Impact Team, the latter of whom are believed to be responsible for the Ashley Madison hacking incident of 2015. It is possible individuals choose to present themselves as a group as it makes them seem more powerful or more threatening, or possibly allows them to deny personal responsibility if they are caught. Similarly, group members may themselves believe the group to be larger than it actually is, or may have an inflated sense of their importance in the group. It has been suggested some members of hacktivist groups such as Anonymous were misled, intentionally or otherwise, into believing they made a substantial individual contribution to cybersecurity attacks, when in fact their contribution towards the success of the attack was minimal or even non-existent[13]. Despite spending extensive amounts of time together online and engaging in shared activities group members may not be aware of each other's real life identity, with attempts to identify individuals (known as doxing) actively discouraged within the group[14]. Perhaps counter to much social psychological theory the anonymous nature of some of these groups may in fact increase stronger communal identity[15].

Within hacker communities and the cybersecurity industry the phrases white, black and grey hat hackers are used to denote motivation. Black hat hacker is used to describe hackers who breach computer security systems for malice or personal gain. A white hat hacker is one who tests computer systems to make them more secure. Such individuals will report any weaknesses they find to the organisation concerned. In doing so they are not breaking any law. Indeed some organisations such as Google will pay monetary rewards to white hat hackers who identify and report weaknesses to them, which are known as bug bounties. It can though be difficult to determine how common such practices are, since companies do not typically wish to disclose to the public or their stakeholders that such a weakness was found to exist in the first place. Between black hat and white hats are grey hat hackers, who may at times engage in illegal or morally questionable action but lack the malicious intent of a black hat hacker. There is a lack

of empirical research in this area and methodological challenges in conducting studies with this population. It was found in one exploratory study[16] that only a small number of participants (9 per cent) self-identified as being a black hat hacker, with the remainder self-identifying as being a white hat hacker (38 per cent), grey hat hacker (49 per cent) or other categories. Participants self-reported motivations primarily related to exposing weaknesses within computer systems, so that they can be fixed, with only a minority reporting that they exploited weaknesses they found for personal gain.

The skills and motivations of the white hat hackers and others who seek to protect systems are highly relevant to the aforementioned career path of ethical security testers. One area in which psychologists can make a contribution is in understanding how to engage such individuals in a dialogue about legitimate cybersecurity jobs and how their abilities may be used for the benefit of society. How to approach these populations is an important consideration. As observed by researchers[14] there are complexities in the motivations and self-identities of those who may be termed hackers, at least in the popular use of the word. Taking an overly simplistic approach in conversations with those who identify as a hacker that implies they are criminally motivated and self-serving should be avoided. It is likely to antagonise groups of people who are in fact highly skilled and who are able and often willing to help organisations fix the gaps within their own cybersecurity.

Understanding psychological manipulation

Many cybersecurity attacks include some form of psychological manipulation of the target. Within the field of cybersecurity and in hacking communities such manipulations are referred to as social engineering, a term that has also been adopted by bodies such as GCHQ and the National Cyber Security Centre. It is important to highlight that this term is used differently than it is in political science or environmental psychology. Although the basic goal of attempting to change social behaviours is often the same. Phishing emails are one of the most commonly used mediums for psychological manipulation in cybersecurity attacks, although there are a range of other approaches that can be utilised in offline and online settings. There is overall a lack of theory based research into psychological manipulation within cyber-attacks, despite many of the techniques used by attackers being based on social psychological processes. Many cyber-attack psychological manipulations make use of the norm of reciprocity[17], which typically takes the form of the exchange of information[18]. Other persuasive techniques are also often employed, along with the exploitation of decision-making heuristics such as providing visual cues in an phishing email (e.g. a bank logo) along with an urgency appeal to push targets into making quick but irrational decisions[19,20].

Social psychological research may inform understanding of these attempted psychological manipulations, despite the relative lack of psychologically informed research studies in this area. Cyber attackers are also known to make use of theories that have less robust support in psychology, such as neuro-linguistic programming[21]. Further exploration of the linkage and conflicts between the psychological manipulations used by attackers and psychological theories may lead to better understanding of where, when and why these attempted psychological manipulations are effective. It is important to note that those who are at greatest risk may not match stereotypes of technological capability. For example, it has been found that it is 18 to 25 year olds, not older people, who are consistently the demographic most susceptible to phishing attacks[22]. There is a lack of research to explain why this may be the case. Research into phishing often focuses on the components of the scam, but not on why such scams work with some individuals and not others[23].

Organisational culture, resilience and change

Organisations are often the targets of cybersecurity attacks, although ultimately the attack still often begins by focusing on individual employees through techniques such as phishing emails. Alternatively individuals may deliberately and knowingly instigate a cybersecurity incident for a variety of reasons including industrial espionage, or as an act of retaliation against a workplace grievance. These risks may be enhanced by the culture of the organisation and attitudes towards cybersecurity. These may vary both between and within organisations. Tallon[24] for example comments that executives often have very different opinions about the value of IT and cybersecurity than those who work within the IT department. Organisational culture and the relationship between the organisation and the employees can be a factor in determining insider threat, in which an individual actively and deliberately takes actions to endanger the cybersecurity of the organisation. There are behavioural indicators and workplace events that can be predictive of insider threats, including stressful events observable in personal and work life, work-related conflicts and sanctions[25]. Organisations often fail to detect these warning signs until an incident has already occurred[25]. This is an area where psychology can make a strong contribution, through better identifying of predictors of future risk behaviours and by providing guidance to organisations on how to support employee psychological wellbeing.

Preventing and mitigating unintentional insider threat can be challenging as it is not easy for an employee to understand what the possible consequences of their actions could be in relation to cybersecurity. To do so may require them to have an understanding of the environment in which they operate, in this case their organisation. Within the cybersecurity domain this is often referred to as situational awareness, with Endsley[26] arguing that there are differing levels.

- Level 1 – Attention or awareness of the elements in an environment.
- Level 2 – Comprehension of the elements into a gestalt understanding of the system status.
- Level 3 – Projection of future system states.

In the case of cybersecurity an individual could be aware that the organisation uses a certain piece of software (level 1). They understand that the software interacts with a database that stores sensitive information (level 2). They realise that an attacker with knowledge of that software could potentially exploit them in order to gain access to information within the database (level 3). Ideally, it could be argued, all individuals within an organisation should have a level 3 situational awareness, so that they can better understand why an attacker may be attempting to get certain information from them and respond accordingly. In reality of course such a level of awareness across an entire organisation could be problematic. A junior employee in a public facing role for example may have very little need to understand the complexities of background company systems, and as such may not feel particularly invested in reaching level 3 of situational awareness. Yet for this very reason such an individual may be an attractive, low risk target for an attacker to attempt to exploit.

There are several government resources available for UK businesses, including Cyber Aware (www.cyberaware.gov.uk) and Cyber Essentials (www.cyberaware.gov.uk/cyberessentials), which are discussed as part of the National Cyber Security Strategy 2016–2021. These resources offer information, self-rating questionnaires and practical advice on how to prevent and mitigate cybersecurity attacks. They are consistent with the research discussed above on how to bring about behaviour change by creating an awareness of risk and offering solutions that can minimise this risk. Nevertheless, there remains a wealth of behaviour change literature from psychology that could be further implemented in this area[27].

Embedding psychological education into cybersecurity training

There has been a shift towards the use of psychological manipulation as part of cybersecurity attacks. This coincides with a time when there is an increasing demand for cybersecurity experts and calls for greater collaboration between practitioners and academics[28]. This presents an opportunity to embed psychology within cybersecurity training programmes and the growing number of BSc Cybersecurity degrees being taught in the UK. A greater knowledge of psychology by cybersecurity practitioners and students may better equip them to understand and address some aspects of cybersecurity. Relevant areas of psychology that can be taught include social psychology, group dynamics, trust, individual differences and the role of emotions when using sociotechnical systems (and how this may link to poor decision-making and risky behaviour). The needs and vulnerabilities of different groups can be explained using psychological research, such as impulse control issues in children and younger adults, or the cognitive deterioration that may be experienced by some older adults. Delivering this content may not be easy. There can be differences in pedagogical, epistemological and ontological approaches to how material is typically taught in Psychology versus Computing departments, and there can be different student demographics within each discipline[29]. Nevertheless, as technological systems become increasingly socio-technical in nature there is a need for greater synergy between disciplines.

References

[1] European Commission (2015). *Special Eurobarometer 423, Cyber Security*.

[2] Klahr, R. et al. (2017). C*yber security breaches survey 2017*. Department of Culture Media and Sport, Ipsos MORI, University of Portsmouth.

[3] Phish Labs (2017). *2017 Phishing trends & intelligence report: Hacking the human*. Phish Labs.

[4] Gibbs, S. (2017). Facebook and Google were conned out of $100m in phishing scheme, *The Guardian*. Retrieved from www.theguardian.com/technology/2017/apr/28/facebook-google-conned-100m-phishing-scheme.

[5] Dahan, M. (2013). *Hacking for the homeland: Patriotic hackers versus hacktivists.* Proceedings of the 8th International Conference on Information Warfare and Security (Iciw-2013), pp.51–57.

[6] McAlaney, J., Thackray, H. & Taylor, J. (2016). The social psychology of cybersecurity. *The Psychologist, 29*(9), 686–689.

[7] Seebruck, R. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation, 14*, 36–45.

[8] Riley, D. (2015, October). 15-year-old script kiddie arrested in TalkTalk hacking investigation. Silicon Angle. Available at https://siliconangle.com/2015/10/27/15-year-old-script-kiddie-arrested-in-talktalk-hacking-investigation/

[9] BBC News (2016). Boy, 17, admits TalkTalk hacking offences. Retrieved 22 May 2017 from www.bbc.co.uk/news/uk-37990246.

[10] Culbertson, D. et al. (2017). *Indeed spotlight: The global cybersecurity skills gap*.

[11] National Crime Agency (2017). *Cyber crime: Preventing young people from getting involved*. 14 June 2017, available from: http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-getting-involved.

[12] Kearney, W.D. & Kruger, H.A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security 61,* 46–58.

[13] Olson, P. (2012). *We are anonymous*. New York: Back Bay Books.

[14] Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy: The many faces of anonymous*. London: Verso.

[15] Tanis, M. & T. Postmes. (2005). A social identity approach to trust: interpersonal perception, group membership and trusting behaviour. *European Journal of Social Psychology, 35*(3), 413–424.

[16] Thackray, H. et al. (2017). *Surveying the hackers: The challenges of data collection from a secluded community, in 16th European Conference on Cyber Warfare and Security.* Dublin.

[17] Happ, C., Melzer, A. & Steffgen, G. (2016). Trick with treat – Reciprocity increases the willingness to communicate personal data. *Computers in Human Behavior, 61*, 372–377.

[18] Tamjidyamcholo, A. et al. (2013). Information security – Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language. *Computers & Education, 68,* 223–232.

[19] Cialdini, R.B. (2009). *Influence: Science and practice* (5th edn, p.xii, p.259). Boston: Pearson Education.

[20] Kahneman, D., Slovic, P. & Tversky, A. (1982). *Judgment under uncertainty: Heuristics and biases* (p.xiii, p.555). Cambridge, New York: Cambridge University Press.

[21] Witkowski, T. (2010). Thirty-five years of research on neuro-linguistic programming. NLP research data base. State of the art or pseudoscientific decoration? *Polish Psychological Bulletin,* 58.

[22] Sheng, S. et al. (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. 2010, ACM: Atlanta, Georgia, USA.

[23] Price, K. & Kirwan, G. (2014). Personality caught in the social net. In A. Power & G. Kirwan (Eds.) *Cyberpsychology and new media: A thematic reader*. Psychology Press: New York.

[24] Tallon, P.P. (2014). Do you see what I see? The search for consensus among executives' perceptions of IT business value. *European Journal of Information Systems, 23*(3), 306–325

[25] Band, S.R. et al. (2006). *Comparing insider IT sabotage and espionage: A model-based analysis*. Software Engineer Institute, Carnegie Mellon.

[26] Endsley, M.R. (2000). *Situation awareness analysis and measurement*. Lawrence Erlbaum Associates Inc.

[27] Davis, R., Campbell, R., Hildon, Z., Hobbs, L. & Michie, S. (2015). Theories of behaviour and behaviour change across the social and behavioural sciences: a scoping review. *Health Psychology Review, 9*(3), 323–344. doi:10.1080/17437199.2014.941722

[28] Richardson, C. (2017). Can the UK deliver where it needs to in digital skills? *New Statesman*.

[29] Taylor, J. et al. (2017). Teaching psychological principles to cybersecurity students. In *2017 IEEE Global Engineering Education Conference (EDUCON).*