**THE SOCIAL PSYCHOLOGY OF HACKERS**

We like to think of ourselves as being individuals who are in charge of our own behaviours and thoughts, especially in countries such as the UK where we have an individualistic culture. However, humans are social creatures. We are strongly driven to be part of groups, and to fit in with what we perceive to be the norm. It is important to note the ‘perceive’ here, because often our perception of what the norm is wrong.

There is a video clip from a candid camera TV show demonstrating classic psychology research in where an individual can be made to engage in some quite odd behaviour simply because everyone around starts behaving that way. The video can be viewed on youtube at https://www.youtube.com/watch?v=dQw4w9WgXcQ

Norms apply in both offline and online settings, and as noted can often be misperceived both by those inside the group and those on the outside. Stereotypes can emerge which may not reflect the true nature and diversity of the group. For example when searching for ‘hackers’ online the most common images that are returned usually convey the idea of criminality.

Cybersecurity is often seen very much as a technological challenge, but ultimately every cybersecurity incident comes down to a series of decisions and actions by people. The technology only facilitates these actions. This is why it is important to understand the psychological aspects of cybersecurity.

There are a number of areas where psychology is relevant in this area. There is the motivation behind the attackers targeting a certain victim, the psychological manipulation of the target (for example through social engineering), the response of victim to being targeted and the overall public perception of cybersecurity. With regards to the latter it can be noted that a cybersecurity attacked does not need to result in a serious data breach to harm an organisation – indeed in some cases the data that is stolen from a company may have very little value. However the fact that a breach was able to occur at all may damage the public reputation of that company.

In recent years hacking has become somewhat glamourized in the media. There is a risk that this could led individuals, especially young people, to become involved in hacking without a realistic understanding of what it entails, or what the risks are. They may overestimate their own abilities, or underestimate the skills of law enforcement and other agencies in being able to identify and prosecute hackers.

There has been some research on the motivations of hackers. Seebruck’s model identifies five broad areas of motivation, with different sub-types of hacker within each area. The closer these sub-types are to the edge of the circle, the more technologically skilled they are. The model demonstrates that hacking is not just about financial gain through criminal activity. Other motivations include prestige, where hackers wish to have the social approval amongst other hackers for being the first person to breach a highly secure system; or hacktivism, where attacks are driven by ideology. From our own research we have found support for the concept of hacking as recreation, where individuals engage in hacking because they find it challenging and enjoyable.

Anonymous are one of the more well-documented hacktivist groups. It was involved in several high profile incidents involving Scientology and the Westboro Baptist Church. It is interesting to note that Anonymous is one of the few hacktivists groups to also hold offline meetings and protest marches. As noted on in the documentary ‘We Are Legion’ many members of the organisation were surprised that other people actually turned up to these offline meetings – many within the organisation had assumed that the size of the organisation had been exaggerated by the members themselves. When meeting face to face (or mask to mask) in real life members also commented on the group being more diverse than they had expected, in terms of age, gender and ethnicity. This demonstrates how the stereotype of a hacker being a teenage boy working in a basement might not be accurate.

Work within Anonymous and other hacker groups has demonstrated several group dynamics processes that would be predicted by social psychological theory.

The infamous Fox News report on Anonymous provides an example of some of these group processes. The news report included footage of an exploding van, which appeared to have little connection to the topic of hacking. This news report could be argued to have galvanised Anonymous into taking further actions, by making them seem far more threatening and powerful than they actually were. Anonymous used this news report as part of their impression management strategy.

Our research has involved exploring the hacking community to gain a better understanding of how these groups operate. This is a challenging area given that many of those involved in hacking are understandably wary of speaking to outsiders. To start with we spent a lot of time observing conversations within online hacking forums. This helped us understand how people interact with each other, and what the norms and etiquette were within each forum. This did varied between forums, depending on their exact focus. We also noted that some forums were quite transient, and rose and fell within popularity over the course of the research.

We then conducted a series of online surveys. The requests to complete these surveys were posted on the online hacking forums. We were upfront about who we were and what the purpose of the research was. Whilst there was some suspicion from the forum users there was, overall, a fairly positive response to our research. Several forum users commented that they were pleased to see researchers taking a serious interest in their community. These interactions led to interviews being conducted with some individuals in order to gain a deeper understanding of the hacking communities in which they are involved. This was done online and also offline, particularly at hacking events such as the DEFCON hacking convention that is held in Las Vegas every July. This event is attended by 20,000 people, and includes people from a wide range of backgrounds.

In one of our surveys we asked people if they considered themselves a hacker. We knew from our time observing the forums that this would be a controversial question, since many people seemed to feel that the term is too vague and has negative connotations. Nevertheless we felt it would be useful to get a sense of how many forums users would identify themselves this way. Just over half of the respondents stated that they saw themselves as a hacker, with a third stating that they did not. This was interesting given that the online surveys were posted on forums that explicitly identified themselves as being about hacking.

We then asked forum users to suggest different names and sub-types of hackers, which we then used as the basis for a question in a subsequent study. This included the terms black hat, white hat and grey hat. A black hat hacker is someone who hacks for entirely criminal purposes. A white hat hacker is someone who hacks for legitimate, ethical reasons, such as for example a penetration tester employed by a company to test their defences. A grey hat hacker is someone who operates between these two points, who may for example engage in some illegal activity in order to demonstrate to an organisation that there are gaps in their security that they need to address.

Grey hat hacker was the most common definition selected by respondents, followed by white hat hacker. Only a small percentage of respondents identified themselves as black hat hackers. We acknowledge that this may be partly due to sampling bias, in that those involved in hacking for purely criminal reasons are less likely to engage with the research. This result was though supported by our observation of forum discussions, interviews and attendance at events such as DEFCON. Overall it seemed that very few individuals became involved in hacking because they had a clear desire to be a criminal. Instead when people did engage in criminal activity it appeared to be more because they had slowly drifted into these activities as they became more deeply involved in hacking.

The age range of respondents fluctuated between respondents in our 2018 vs 2017 surveys, but the overall pattern remained consistent. It is of note that the most common age group was those aged 26 – 35, with a number of people in the older age groups. As one interview participant commented many of the people who began hacking in the 1980s and 1990s are now older and have legitimate careers, but are still involved in hacking.

The results from both surveys indicate that hacking is a very male dominated community, which reflects the gender imbalance in the cybersecurity profession. That being said several participants in our research stated that whilst they are female they would pretend to be male in hacking forums, since disclosing themselves to be female would often result in being negatively targeted by other forum users. The research team also observed that the gender balance at events such as DEFCON was – although still male dominated – more equal than perhaps could be expected from the online forum discussions.

There were a range of opinions amongst participants around whether online security should take priority over personal privacy. There was more agreement over the idea of hacking involving trying to find flaws and weaknesses in systems. The majority of respondents also agreed that it was important to expose flaws and weaknesses in systems. This especially appeared to the case when it involved a system run by a large organisation who should have the resources necessary to protect information, and in particular customer/ public data. However, the majority of respondents did not believe that it was appropriate to exploit any flaws they found.

These results were reflected in the interviews and discussions at hacking events. Participants expressed frustration at organisations often failing to take the basic steps necessary to ensure that their systems are secure. They also spoke of times when they had made a company aware of a flaw in their systems but no action was taken; or the flaw was subsequently fixed but the hacker who identified the issue received no thanks or acknowledgement from the company.

Many participants spoke of hackers being fundamentally different from non-hackers in some way. They felt a key characteristic of hackers was to want to understand how things work, and to test the limits of what systems can be made to do. They noted that this is what one of the early definitions of a hacker is, and does not imply that anything criminal is taking place.

There is a lack of research on if there really is a fundamental difference in the cognitive style of hackers vs non-hackers. Our interpretation was that whilst there were some traits that appeared to be common amongst hackers there is insufficient evidence to conclude that there is a consistent and strong difference in cognitive style between hackers and non-hackers. It is possible that this perception of hackers being somehow different from everyone else is a view that is exaggerated by the community itself, in order to create a sense of being unique. This relates back to the discussion put forward earlier on the role of self-esteem and impression management within groups. There are though some organisations that specifically target people on the autistic spectrum for cybersecurity roles, in the belief that their characteristics make them especially skilled in this role.

There was a lot of debate between participants on how someone comes to be seen as a hacker. Some felt that this was a status that the community had to confer on an individual, whereas others felt that this was something people could decide for themselves. There was also disagreement over the validity of the distinction between black, grey and white hat hackers. Several participants commented that they felt it was impossible for someone to become a hacker without having at least some involvement in criminal activity.

Participants identified trust as a key issue within hacking communities. Trust was seen as something that had to be earned. Forum users were very wary of anyone who asked for advice on how to do something if that person did not first of all demonstrate that they had made a concentrated and genuine effort to solve the problem themselves first. Nevertheless, there were also some inconsistencies in how trust was implemented and how it was discussed. For example, several individuals who ran hacking forums stated that they do not place their trust in anyone – yet (when prompted by the researchers) would acknowledge that they do exhibit trust through for example giving moderators power within their forums.

One clear finding from the research was that they vast majority of people on hacking communities do not have criminal intent. This is not to say that all hacking is well-intended, or that those with criminal intent do not exist. In addition people within law enforcement or other organisations may have a different opinion than hackers on how harmless some of the more grey hat hacking activities actually are. However overall it would seem that those with malicious intent are in the minority. Instead the main motivation for hacking is a passion for understanding systems and for testing the limits of these systems. There is frustration within the communities over systems which fail to take basic security precautions, especially systems operated by large organisations that have the responsibility for public or customer data. There is a willingness within hacking communities to engage with organisations and the public to address these flaws – but this is a relationship that must be based on mutual respect and trust.

The overlap between psychology, hacking and social responsibility is being increasingly recognised. The research team were invited to share their results at the Social Engineering Village at DEFCON in July 2017, which was a standing room only event. This event was led by famed social engineer and cybersecurity expert Christopher Hadnagy, who had previously authored the book ‘Social Engineering: The Art of Human Hacking’. As a result of the increasing awareness of the role of psychological research in cybersecurity Hadnagy’s latest version of his book has undergone an important change – it is now entitled ‘Social Engineering: The Science of Human Hacking’.

As part of the work the research team have recently produced a British Psychological Society briefing paper on the role of psychology in cybersecurity. This paper notes the increasing cybersecurity skills gap and argues that there is a need to more strongly engage with hacking communities, and in particular young people who have an interest in hacking. This will provide opportunities to steer such individuals towards legitimate cybersecurity careers where they can use their passion and skills for the social good.

There are additional areas where psychology can contribute towards cybersecurity. This video demonstrates the use of eye-tracking technology to understand how people process phishing emails and websites. In this case it can be seen that the participant barely looks at the address bar of the website, which would have given them an indication that the site they were on was actually a fake one.

The research team are involved in a range of other projects across Dorset.

Beginning in 2017 we began a yearly conference that aims to bring together individuals and stakeholders with an interest in the psychological and behavioural aspects of cybersecurity. Our next event will be in September 2019 at Level 39 of CybSafe in One Churchill Place at Canary Wharf. This event is open to all.