The reality of 'cyber awareness': findings and policy implications for Scotland

A Scottish Justice Fellowship Briefing Paper

Dr Shane Horgan
Edinburgh Napier University

This publication is produced by SCCJR The Scottish Centre for Crime & Justice Research

Executive Summary

This briefing paper represents a summary of doctoral research that explores how different groups make sense of and respond to cybercrime in their everyday lives. The research found that people from different groups, places, and times think about cybercrime and cybersecurity in different ways. This has implications for government and police awareness raising campaigns. Population-level awareness campaigns designed to communicate 'simple' messages may get lost in translation or disregarded because they do not resonate with the social and cultural contexts of their target audiences. After considering the challenges government and police face, the report imagines possible future directions for cybersecurity awareness raising that may enable them to be more sensitive to local social cultural contexts and foster the creation of communities of supportive cybersecurity.

Key findings

- Current public facing responses to cybercrime prevention are predominantly focused on raising awareness and behaviour change. These campaigns rely on people interpreting messages and risks in the same way and coming to the same 'rational choice' based conclusion.

- This research found that people think about cybercrime and interpret the risk it poses to them in different ways. This may lead to them feeling that government and police driven cybersecurity messaging is irrelevant or unhelpful to them.

- Awareness campaigns risk creating a hostile environment for victims by focusing on individuals' failures to take steps to secure themselves, and neglecting the wrongdoing of offenders, or the harm of the offence.

- This may lead people to avoid engaging with technologies and services that could improve their quality of life. Equally, stigma will negatively affect people's willingness to report cybercrime or seek support when they need it.

- Some participants expressed a reluctance to report cybercrime to the police except in very specific circumstances. They struggled to fit cybercrime into their understanding of the police role and questioned whether they were the appropriate agency to report to.

1. Introduction

Home to a vibrant digital economy, the continued prosperity of Scotland necessitates resilience to a vast cyber-threat landscape. However, the Internet presents significant challenges to conventional state modes of regulation. Offences are vast in number, offenders are hard to identify and difficult to reach, victims are accessible 24/7 and police are under-resourced and ill-equipped to respond to mass-victimisation events which characterise major cyber-incidents.

A recent review of evidence produced by the Scottish Government (2018) and the introduction of cybercrime recording to the Crime Survey for England and Wales illustrates how serious the problem is; cyber-offences now outnumber more conventional crimes. Tackling the cybercrime problem necessitates drawing a range of actors together to engage in crime prevention. Getting individual users ("the public") on board represents one of the major contemporary cybersecurity challenges of our time.

'Awareness' is a centrepiece of the Scottish Government's Learning and Skills Action Plan for Cyber-resilience 2018-2021. It aims to change the public's behaviour in a way that reflects the array of online risks to which they are exposed. Academic research exploring public responses to cybercrime is lacking, although gradually gaining momentum. This research attempted to address this gap by discussing cybercrime and cybersecurity practices with different groups of people. This allowed me to examine 'cyber-awareness' and its functions in the real-life contexts it is intended to reshape.

This briefing will reflect on the findings of that research and explain their relevance to cyber-resilience work. In the first two sections below, I critically analyse the efficacy of awareness campaigns and describe how folk knowledge and the language of awareness messages may negatively affect people's security behaviours. In the final two sections of the piece, I reflect on the extent to which the police were perceived as the appropriate agency who could, or should, respond to cybercrime. Last, I consider the wider societal context in which efforts to raise awareness take place and what this means for cyber-awareness raising efforts.

2. Method

The research project focused on two central research questions:

1. **How do people make sense of and feel about cybercrime?**
2. **How do they respond to it in their everyday lives?**

Focus groups and interviews were employed to generate discussions about cybercrime and cybersecurity with different groups of people: university students, parents with school aged children and older users. These groups were selected for the varying patterns in internet use across demographics, as well as the diversity of experience and concerns about technology likely to emerge. The findings discussed below draw on empirical data from 5 focus groups (4-8 participants) and 13 semi-structured interviews distributed relatively evenly across each of the participant groups.

While the research employs a reasonable sample of people for a qualitative study of this nature and achieved 'saturation' before concluding the fieldwork, the feelings and beliefs described here are not suggested to be generalisable to the wider population. Nevertheless, the findings are generally supported (with some interpretive analytic differences) by larger quantitative and mixed methods work conducted later by the NCSC (2019) whose findings were similar, but interpretations differed.

3. Background: The Limits of 'Awareness Raising'

The underlying assumption of awareness campaigns is relatively simple. By informing the public about a risk (e.g. smoking, drinking and driving, or illegal downloading) and what they need to do to manage that risk (stop smoking, wear seatbelts, and don't download copyrighted material), people will incorporate this new information into the way they understand the world and adjust their behaviour accordingly. In an ideal scenario, people adapt their behaviours to achieve the outcome that is in their best interests: the 'rational choice'. In the context of criminology and crime prevention policy, this perspective is more commonly applied to the design of interventions aimed at altering the behaviours of potential offenders rather than potential victims (see Cornish and Clarke, 2006).

While people operate with a degree of rationality, it is poor grounds on which to assume the public(s) can be driven to act, and indeed many of the previous examples rely on a complex apparatus of 'enforcement'. In their everyday lives people tend not to approach every decision with a cost/benefit analysis. People also regularly come to very different conclusions about what the 'rational choice' to make might be in different situations. Therefore, how people make sense of the risk posed by cybercrime is shaped by a wide range of social, cultural, and economic factors that vary from person to person, place to place, and over time (Bada et al., 2015). This means that any approach to changing a population's behaviour needs to at least acknowledge the heterogeneity of the population it is supporting, or at best specifically tailor its messaging to resonate with different groups within those populations. If messages are not sensitive to the contexts of individuals they are intended to reach, they risk being disregarded or ignored.

A confounding problem in this context is that 'security' and security behaviours have the burden of being 'intangible' (Loader et al., 2015). The cost of security is one thing, but if functioning correctly, one might never know just how effective or 'worth it' their investment was. It is hard to evidence what has not happened because of your motion-sensor lights or stronger account password. What is tangible is the persistent costs and inconveniences that security measures often impose on employees trying to do their jobs effectively, or people simply going about their everyday lives.

The analysis of focus group and interview data presented here illustrates how cultural representations of cybercrime, 'hackers', and 'ideal victims' limited the effectiveness of awareness messages and shaped how everyday security behaviours were enacted. Most importantly, these were most often in ways that awareness messaging did not anticipate. The central point here is that awareness messages are not communicated and interpreted in a cultural vacuum, and they necessarily contend with pre-existing beliefs, news media, fiction, and stories from family and friends (Radar and Wash, 2015; Wall, 2012; 2007).

It also reveals some negative and possibly harmful consequences of awareness messaging for actual or potential victims. The findings suggest that awareness campaigns risk producing a hostile climate for victims by focusing more attention on their 'wrongdoings' than those of offenders. This constructs victims or potential victims as blameworthy which may negatively impact reporting or help-seeking. Instead campaigns may consider reframing messages that are geared towards fostering local communities and networks of support rather than highlighting individual risk and responsibility.

4. Findings And Policy Implications

The following sections will discuss in more detail the themes that emerged from the analysis of both the focus group and individual interview data.

4.1 Social and Cultural Implications

Knowledge about crime is imparted in a complex social and cultural environment. There are a vast range of influences and sense-making varies from group to group.

The research participants were mostly aware of the risk cybercrime posed and thought it was a serious problem. Mirroring recent research findings from the Home Office (Home Office, 2018) and the NCSC (National Cybersecurity Centre, 2019), people held beliefs about risk that contradicted official accounts and warnings about crime. Their beliefs and feelings were informed by media imagery, fictional representations of 'hackers', and 'common folk knowledge' which tends to percolate across our many social networks. These sources of information prevailed over 'official narratives' in shaping the participants sensibilities towards cybercrime.

In the case of university students, they often felt they did not fit the correct 'victim' profile to warrant concern. They perceived themselves as insufficiently 'worthwhile' targets. They had little of value to lose, and some suggested that, even if they did, there was little they could do to defend themselves. Despite being aware of and believing cybercrime was a serious problem facing society, they interpreted the risk it posed as of little relevance to them. This negated the need for ever vigilant security-oriented action.

"It didn't really bother me because it wouldn't have any effect on my life at all and I have nothing to hide in that way. So…?"
(University Student, Interview)

The parents interviewed were security active and security conscious, but often felt 'they could do more', both to protect themselves and to protect their children online. Parents were very cognisant of pressures to be ever vigilant, and discussions of individual successes and failure tended to reverberate around school yards and social networks.

Some reported that where parents were seen to be irresponsible or 'too relaxed', this would impact on the extent to which their children were included in wider activities. Nevertheless, most suggested that the demands made of them to be secure sometimes conflicted with other pressures, both practical and value based. Parents navigate an impossible set of demands, and perpetual surveillance of their children's online activity was simply lower on their list of tasks and responsibilities. Some parents felt excessive security would threaten what they wanted their family life to be like and resisted turning their family into a 'boot-camp'. Others wanted to protect their children's 'innocence' from uncomfortable conversations about the threats and risks they might face. There are also more practical and technical issues at play. Security-technologies intended to protect children were suggested to be cumbersome, too limiting, or introduced what was felt to be an unreasonable degree of inconvenience to maintain.

"Perhaps we could be a bit more organised and systematic than that [with security], but then you know family life not always organised, it's not a boot camp, and nor should it be"

There was a clear sense from the data that the security expectations and pressures with which parents felt confronted lacked an appreciation of their lived experience. They tended to suggest that meeting them was mostly irreconcilable with the reality of everyday family life and raising children. As a result, they developed their own tailored domestic 'cybersecurity projects' which reflected what they felt was reasonable and achievable in terms of security, while maintaining a harmony at home and ensuring their children weren't excluded from their social networks as a result.

Last, and in contrast, older users who participated seldom believed they needed to worry about cybercrime directly. This was because they felt they did little online which might lead them to be victimised. They argued that, as older people, they were particularly vulnerable and were concerned that they would 'make a mistake' or be targeted. As a result, many limited their activity to avoid the risk entirely. The activity they did engage in, and felt comfortable with, seemed so distant from younger people's uses, they felt they need not be concerned. For them, cybercrime was an issue for the 'young' music downloader and tech savvy 'eBay user'.

"Because I'm… Ok, I get worried in case I make a mistake […] Stupid things, you know. I don't want to make a mistake and create hassle for anybody else, that's the main reason [for not using services]. I mean, if I need anything my daughter has an Amazon account[…] and she can get it for me"
(Older user, Interview)

When it came to engaging in any activity they interpreted as potentially risky, many relied heavily on the support of their families and community groups to navigate or shoulder those dangers.

If they did not have people to rely on to support their online tasks and goals, they risked being marginalised and excluded. Older users had clearly interacted with official awareness messages but interpreted them in an unexpected and potentially problematic way. Several older users suggested that the 'simple steps' to be secure echoed in awareness messages were not so simple or straightforward for them. This led a number of older users to feel less secure or able to manage online risks. Perhaps more worryingly, they were acutely aware of the pressure on individuals to be personally responsible for their own safety online. As a result, they often avoided using services that would allow them to maintain their autonomy or improve their quality of life.

4.1.2 Implications For Enhancing 'Cyber-Resilience' in Scotland

The nature and scale of behaviour change that the cyber-resilience strategy aims to achieve is significant in that it is goal is to reshape how people think about the risk posed by cybercrime and to change behaviour at a population level. This research suggests a number of clear implications for enhancing cyber-resilience:

Different groups will require different messages that are sensitive to their social and cultural context and reflect the practical realities of their everyday lives and feelings about cybercrime. If these campaigns are to improve their effectiveness and reach, the differences between social groups need to be acknowledged. While there is clearly a limit on the extent to which messages can be tailored at a national level, there is a lack of research available to inform the development of even higher-level groups. Further work is required to identify the efficacy of different messages and the extent to which they resonate with different groups of the population.

Awareness campaigns need to be sensitive to the way they frame the issue of victimisation to avoid stigmatisation and victim blaming. This is particularly important in a context where many individual victims have been exposed in a data breach, which is far beyond their control. It is well established that in pursuing an agenda of 'individual responsibility for crime prevention' (see Button and Cross, 2017), an atmosphere is created which is hostile to victims. In the absence of offenders who are often far beyond the reach of the state, our focus is turned on the mistakes of victims which are quickly equated with deviance. An atmosphere of this nature will will risk leaving individuals fearful of stigmatisation and reputational damage. This will negatively impact willingness to report cybercrime or to seek support. Equally, as in the case of older users, it will dishearten and deter people who would benefit significantly from the affordances of information technology and online services. At the time of writing, Scotland is in phase one of emerging from the lockdown triggered by the Sars-CoV-2 pandemic. In this context, enabling older and vulnerable users to engage with information technology safely has never been more important (for more detail see Collier, Horgan, Jones and Shepherd, 2020).

Cybersecurity is an inherently collective good, and arguably placing emphasis on supporting the cybersecurity of one another is a more profitable approach, or perhaps simply less harmful. Thirdly, it is also worth questioning whether targeting feelings of risk or fear of victimisation is productive. Rather than appealing to individuals' feelings of 'fear' (for a more extensive discussion Renaud and Dupuis, 2019), a change of tactics. might be required. In previous renditions of 'responsibilities' for crime prevention such as 'neighbourhood watch', police instead tapped into people's sense of collective responsibility and efficacy. Cybersecurity messages rarely make connections between the value of individual security and the security of one's family, friendship groups and wider community which some research suggests is the primary vector for security information and advice (Radar and Wash, 2015).

4.2 Public Understandings of the Police and Reporting Cybercrime

Beyond individuals taking private action themselves, a further aspiration in Scotland is to encourage the reporting of certain cybercrimes to the police via 999 or 101. A recent review by the Scottish Government (2018) highlighted the continued problem of low reporting of cybercrime to both police and the dedicated national reporting centre Action Fraud UK. There are several common explanations for this also mentioned in this report; a perceived lack of seriousness, a perceived lack of harm, unawareness of victimisation, belief that the police will not do anything. These explanations generally reflect the underlying challenges for the criminal justice system in responding to the global nature of cybercrime, for instance multi-jurisdictional, investigative costs, limited available expertise, high volume, public demand (See for example, Yar and Steinmetz, 2019; Wall, 2008).

The public may well be aware of the limits of the police to respond to cybercrime. However, it may also be that cybercrime simply does not align with the public's understanding of the police, what their job really is, what they are for, and what needs to happen to justify calling them. In Robert Reiner's classic account of policing, The Politics of the Police (2010), the ability to respond rapidly ('emergency') and to maintain public order is of central importance to the public. They are equipped to do so by virtue of their capacity to use force in the event it might be necessary, even if this requirement is rare and mostly avoided.

My interviewees articulated specific circumstances in which calling the police in the case of cybercrime would be straightforwardly appropriate. These cases tended to be those that the public routinely express a high demand for response; for example, sex offences, terrorism, crimes involving children (See Yar, 2013).

Other key criteria included an identifiable and proximate offender, where there was an immediate risk of further harm, and that police intervention could reasonably be expected to prevent it (i.e. the need for an emergency response). Many participants struggled to imagine situations in which they themselves might call the police if they were victims of more mundane and routine cybercrimes (e.g. malware, phishing), suggesting the police were for 'more serious' incidents. A number of participants from different groups suggested that they resisted reporting cybercrime due to the potential stigma they might experience, or because they felt their victimisation 'was their own fault'.

The rapid, commanding, and potentially coercive response of uniformed officers is a potent symbol of 'the police' and what they do. The experience of common cybercrimes emerged in the data as something normal and 'part of using the internet'. As a result, it seldom fitted into the public's imagination of the police, and this understanding shaped participants' reporting behaviour. The experience of cybercrime is one that doesn't have an obvious physical place or space, like the street, the school or the pub, nor does it have a visible offender who might be within reach of beat officers. This likely inserts further conceptual distance between cybercrime, the police, and the public's traditional understanding of routine policing. To confound this issue further, many interviewees described a range of other agencies or actors who they felt were more appropriate 'first responders' and indeed more appropriate sources of advice; banks, computer repair stores, or internet service providers and platforms.

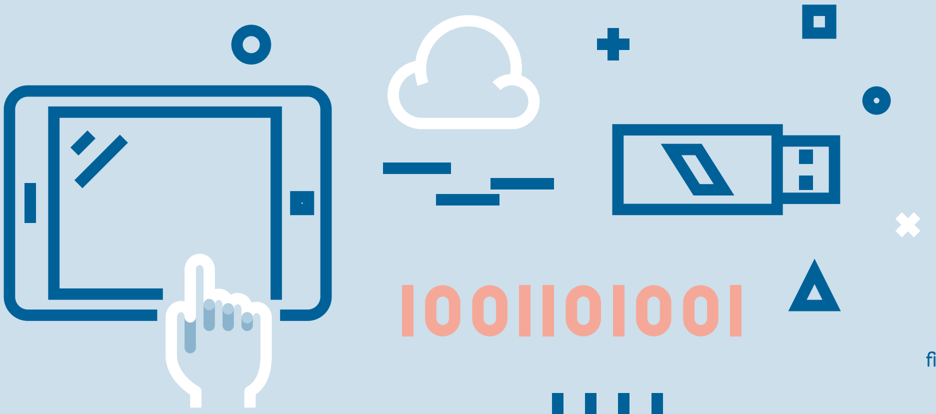
4.2.2 Implications for Policy And Practice

There are several recommendations that might be drawn out from the above discussion. Awareness messaging needs to do more than attempting to change behaviour.

First, beliefs about the role and mandate of the police are embedded in our culture, and what people feel it means to dial 999 or 101 may well represent a further challenge to reporting if Police Scotland are to be a central point of contact for recording. **One step towards improving reporting will involve challenging the assumptions people have about when the public can and should call the police about cybercrime.**

Beyond raising awareness of risks and appropriate security behaviours, campaigns may also need to challenge the public's understanding of cybercrime as a private issue, resolved informally by formatting a computer or seeking the help of friends or family. In this way, **awareness messaging from both Scottish Government and Police Scotland should set out what types of cybercrimes should be reported by the public (e.g. malware, phishing), under what conditions (e.g. successful, attempted, reported to bank or service providers), how it should be reported (e.g. online, via 101 or 999)** and the procedural steps towards justice that possible victims might expect if they were to submit a report. This also means clarification of the public police role in cybercrime policing at a more local level.

Overall, it is prudent that we challenge the status of cybercrime as a 'normalised aspect



of internet use' to be solved by private market solutions and family or social networks. **Cybercrime needs to be reconstructed as recognised harm done to individuals that deserves both the attention of police and individual access to justice.** Doing so may itself represent a 'simple step' towards improving reporting and reducing the stigmatisation of cybercrime victims.

4.3 How Online Life Impacts Cyber-Awareness

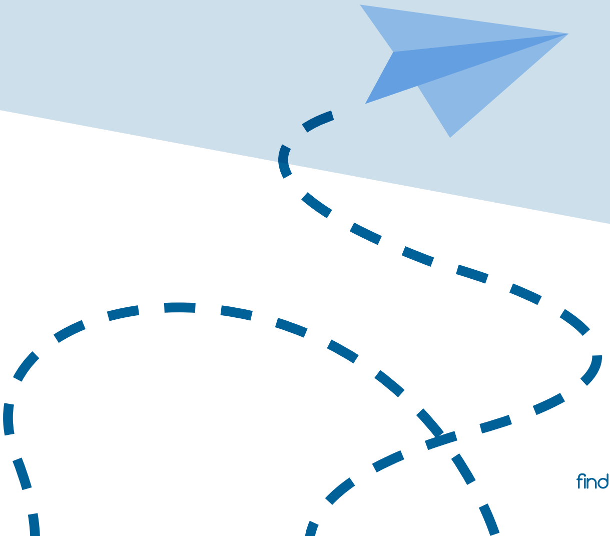
Last, there is the issue of the wider technological and cultural context in which we live. As Bada, Sasse and Nurse (2015) point out, if awareness campaigns do not resonate or fit into the target audience's 'cultural system', they are more likely to fail. Beyond cybercrime, contemporary society does little to embed the notion that personal data is our own, that it is valuable and that it is worth protecting. Embedding this value in everyday life may be a precondition of more lasting cyber-resilience oriented behaviour change.

We need to teach people the value of their own personal data and why it is worth protecting

Awareness campaigns may improve people's knowledge of threats to their safety online and their awareness of the steps required to mitigate those threats. However, we do little as a society to teach people the value of their own personal data and why it is worth protecting in the first place. Instead, it is normal to trade personal data and privacy for convenience. For example, refer to the university students mentioned earlier who questioned the value of what they were protecting and why anyone would be interested in victimising them. Their questions about 'what's the worst that can happen', and assumptions that their data was probably 'already out there anyway' reflect this problematic and damaging situation.

We need to continue to challenge the free and irresponsible trading and storage of personal data and de-normalise the undermining of individual privacy

What does this mean for awareness? Essentially, it is worth questioning whether government, police, and indeed wider efforts to change public behaviour are somewhat in vain while we continue to live in a society that freely trades in personal data acquired insidiously, and one that undermines personal privacy at every digital corner (Zuboff, 2018). Perhaps, in tandem with making people aware of the risks cybercriminals pose to their data, awareness raising work also needs to highlight that personal data is important, valuable and worth protecting. While efforts to enforce greater regulation on corporate accumulation and storage of personal data (e.g. GDPR) have certainly gathered momentum, data breaches and irresponsible data hoarding continue to undermine the efforts of individuals to take 'simple steps' to secure themselves.



5. Conclusion

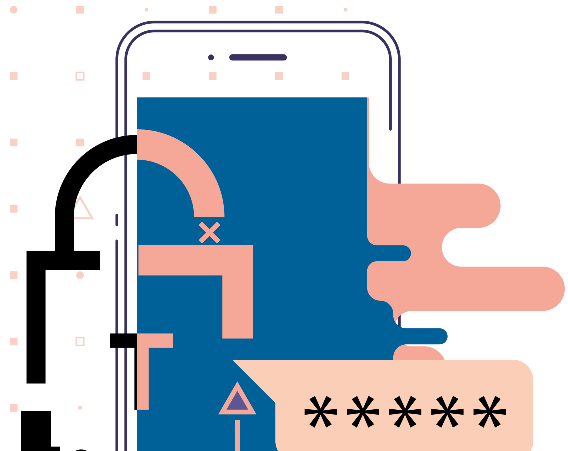
This briefing paper has described, drawing on empirical data collected between 2016 and 2018, how different groups of people make sense of and respond to cybercrime in their everyday lives. The research found that population level awareness campaigns designed to communicate ‘simple’ messages may get lost in translation or disregarded because they do not resonate with the social and cultural contexts of their target audiences. Equally, awareness messaging tends to emphasize individual responsibility and efficacy, rather than acknowledging the wrongdoing of the offender, harm of the offence, or fostering a sense of collective efficacy and communities of support. An unintended consequence of emphasizing individual responsibility is the creation of a hostile or stigmatising environment for victims which could negatively impact reporting and limit access to justice. These findings have led to the development of several recommendations for cyber resilience building activity among policy makers and police services.

Key Policy Recommendations

- Different groups will require different messages that are sensitive to their social and cultural contexts and reflect the practical realities of their everyday lives and feelings about cybercrime.

- Awareness campaigns need to be sensitive to the way they frame the issue of victimisation to avoid stigmatisation and victim blaming.

- Cybersecurity is an inherently collective good, and arguably placing emphasis on supporting the cybersecurity of one another is a more profitable approach, or perhaps simply less harmful.



- More specific and accessible guidance on how and in what instances the public should report cybercrime to Police Scotland should be provided in order to challenge the assumptions people have about when the police role in responding to cybercrime.

- Cybercrime needs to be reconstructed as a recognised harm done to individuals that deserves both the attention of police and individual access to justice.

- Public awareness of the value of their own personal data and why it is worth protecting in the first place need to be improved.

- The free and irresponsible accumulation, trading and storage of personal data needs to be challenged and the undermining of individual privacy de-normalised.

References

Bada, M., Sasse, A. and Nurse, J. (2015), 'Cyber Security Awareness Campaigns: Why do they fail to change behaviour', Proceedings of the International Conference on Cyber Security for Sustainable Society, Available at: https://arxiv.org/abs/1901.02672 [Accessed: 27/05/2020]

Button, M. and Cross, C. (2017) Cyber Frauds, Scams and their Victims. London: Routledge

Collier, B., Horgan, S., Jones, R. and Shepherd, L. (2020) 'The implications of the COVID-19 Pandemic for cybercrime policing in Scotland', The Scottish Institute for Policing Research, Available from: http://www.sipr.ac.uk/publications/pandemic-briefings [Accessed: 02/06/2020]

Cornish, D. and Clarke, R. (2006) 'The rational choice perspective', in Henry, S. and Lanier, M. (eds) The Essential Criminology Reader. Boulder: Westview

Home Office (2018) 'A Call to Action: the Cyberaware perceptions gap', Available from: https://www.gov.uk/government/publications/cyber-aware-perception-gap-report [Accessed: 06/03/2019]

Horgan, S (2020) Cybercrime and everyday life: exploring public sensibilities towards the digital dimensions of crime and disorder. PhD thesis, University of Edinburgh.

NCSC (2019) 'UK Cyber Survey' [Internet] Available from: https://s3.eu-west-1.amazonaws.com/ncsc-content/files/UK%20Cyber%20Survey%20-%20analysis.pdf [Accessed: 02/06/2020]

Rader, E., & Wash, R. (2015). Identifying patterns in informal sources of security information. Journal of Cybersecurity, Vol.1(1): 121-144

Scottish Government (2018) Cyber crime in Scotland: evidence review. Available from: https://www.gov.scot/publications/cyber-crime-scotland-review-evidence/ [Accessed: 27/08/2020]

Wall, D. (2012) 'The Devil Drives a Lada: the social construction of hackers as cybercriminals', in Gregoriou, C. (ed) The Construction of Crime. London: Palgrave

Wall, D. (2008) 'Cybercrime and the culture of fear', Information, Communication and Society, Vol.11(6): 861-884

Wall, D. (2007) Cybercrime: the transformation of crime in the information age. Cambridge: Polity

Yar, M. and Steinmetz, K. (2019) Cybercrime and Society. (3rd edition) London: Sage

Zuboff, S. (2018) The Age of Surveillance Capitalism. London: Profile Books

Contact Information

S.Horgan2@napier.ac.uk

The full research thesis from which this briefing derives is freely available online:
https://era.ed.ac.uk/handle/1842/35869

Scottish Justice Fellowships are a collaboration between the **Scottish Government, Scottish Centre for Crime and Justice Research (SCCJR)** and **Scottish Institute of Policing Research (SIPR)**. Fellowships fund leading doctoral researchers near or recently completing PhDs to translate their work into accessible outputs aimed at policy and practice audiences. Views expressed are those of the author and do not necessarily reflect those of SCCJR, SIPR or the Scottish

SCCJR The Scottish Centre for Crime & Justice Research

The Scottish Institute for Policing Research

Scottish Government