The Portsmouth Cybercrime Awareness Clinic Project:
Key Findings and Recommendations

October 2019

Authors: Dr Vasileios Karagiannopoulos
Dr Lisa Sugiura
Dr Annie Kirby

© 2019 Institute of Criminal Justice Studies, University of Portsmouth
# Contents

Acknowledgements 2

Foreword 3

1. Executive Summary 4

2. Introduction 6
   2.1 The Project 6
   2.2 Background 6
   2.3 Aim and Objectives 8

3. Summary of key findings and conclusions 10
   3.1 Public Engagement 10
   3.2 Research with Children and Young People 12
   3.3 Research with Older People 15
   3.4 Research with Small and Medium Organisations 17

4. Next Steps and Overall Conclusions 20
   4.1 Next Steps 20
   4.2 Conclusion 20

Appendix A - Stakeholder Map 22

Appendix B - References 23

Contact Information 26
Acknowledgements

The Cybercrime Awareness Clinic team consisted of:

**Dr Vasileios Karagiannopoulos**
Director of the Cybercrime Awareness Clinic and Reader in Cybercrime and Cybersecurity

**Dr Lisa Sugiura**
Deputy Director of the Cybercrime Awareness Clinic and Principal Lecturer in Criminology and Cybercrime

**Dr Annie Kirby**
Research Associate, Cybercrime Awareness Clinic

Additional support for public engagement and research activity was provided by student volunteers who were either final year undergraduates or master’s degree students in a criminology- or cybercrime-related field.

The clinic team would like to acknowledge Hampshire Constabulary and the Office of the Police and Crime Commissioner in Hampshire, not only for their financial support, but also for the advice, expertise and resources generously shared throughout the course of the project. This publication reflects only the views of the authors.

We would also like to acknowledge the contributions of all the organisations, individuals, schools and colleges that have collaborated with the clinic, taken part in public engagement activities or research, or supported the clinic project in other ways over the past two years. The clinic project would not have been possible without your time, commitment and expertise.
Cybercrime is increasingly part of our public consciousness. But the opportunities enabled by greater digital connectivity also create risks, and the level of awareness of those risks is not always clearly articulated or understood. Keeping people safe and identifying people who need our help are core parts of our policing mission. Doing this effectively to prevent people from becoming unnecessary victims of crime, and protecting people from becoming repeat victims, are critical parts of the combined fight against cyber criminals. Policing must be part of this solution but by no means is it a responsibility we shoulder alone.

There are a number of questions we need to address: how do we raise cyber awareness in our communities and increase community cyber resilience? How should this be achieved effectively, in ways that are simple, clear, sensible and practical in what can seem like an impossibly complex landscape?

That’s why Hampshire Constabulary commissioned the University of Portsmouth to undertake a fixed period of funded research to help identify good practice in where to target cybercrime awareness, to whom, through which methods, by whom and over how long. Answers to these important questions, arrived at through this research, are now helping us steer our multi-agency protect response with greater confidence and clarity.

Ben Snuggs
Assistant Chief Constable (Crime, Criminal Justice and Intelligence)
Hampshire Constabulary
1. Executive Summary

The Cybercrime Awareness Clinic was a 2-year project based in the Institute of Criminal Justice Studies, University of Portsmouth, funded by Hampshire Constabulary. The project aim was to develop and pilot an innovative research and collaboration space to help raise awareness of and build resilience to cybercrime among the local community and organisations.

The project had three main strands. First, the goal was to provide advice to vulnerable groups in the local Portsmouth community, focusing mainly on young people in schools and colleges, small and medium organisations (SMOs) and older people (60+). Second, the clinic aimed to increase the knowledge of the cybercrime threats and risks that relate to the above populations. The third strand of the clinic related to developing a transferable model for the implementation of cybercrime awareness clinics in other parts of the country.

This report includes all the developments and findings generated during the two years of the project. The increase of cyberawareness through stakeholder engagement has been very successful, gradually enabling us to access the desired research populations and to make contact with more diverse and minority groups not initially part of the research plans. For example, we have supported victims of domestic abuse and engaged with community groups providing services to disabled and BAME people. While this has created additional, unanticipated workloads, it has allowed the clinic to develop further. The clinic has expanded its reach in the community, as well as inspiring plans to work further with these groups and others, including the LGBTQI+ community.

The research aspect has also been successful, despite significant challenges in engaging potential participants, especially schools/colleges and SMOs. Through the research, we have managed to provide a clear snapshot of the threats that the vulnerable groups we have engaged with face. We have also advised on improving local practice and changing local processes to assist the different stakeholders involved and our partners in tackling cybercrime threats and helping victims of cybercrime more efficiently. The strength of the pilot research the clinic has completed is reinforced through the combination of findings from the different types of community groups in conjunction with active reflection from our public engagement experience and a review of relevant literature.

Operating as the local cybercrime awareness clinic for two years has been an eye-opening and multi-faceted experience. The project unfolded organically and unexpectedly in areas and ways that were not initially anticipated. Many ideas that seemed great on paper, did not work as well in practice and many new ideas were formulated and realised as the project grew and took shape. The clinic team has developed an extensive list of challenges faced and lessons learned, together with best practice recommendations. We expect these recommendations to inform future initiatives and, although we understand that some of these challenges relate to the particular organisations involved or the location this project has
taken place in, we are confident that the overarching messages are applicable to most environments and organisational synthesises.
2. Introduction

2.1 The Project

The Cybercrime Awareness Clinic was a 2-year project based in the Institute of Criminal Justice Studies, University of Portsmouth. It commenced in April 2017 and was funded by Hampshire Constabulary. The clinic was conceived as a multi-stakeholder, interdisciplinary project with the aim of filling a gap in cyberawareness education locally. It aimed to develop a more holistic, bottom-up understanding of the risks and needs of the public and increasing awareness and resilience against cybercrime for vulnerable local residents and small and medium organisations (SMOs) in Portsmouth and the surrounding area.

This report summarises the project and its achievements and findings up to the end of its pilot phase.

2.2 Background

The project unfolded during a period that saw cybercrime continuing to be an important issue of public protection policy and an increasingly significant issue for communities and businesses at a national level.

In the year ending March 2018, Action Fraud – the UK’s national reporting centre for fraud and cybercrime – recorded just over 740,000 fraud-related crimes, of which 86% were cyber-enabled, and a further 23,500 cyber-dependent crimes.¹ In terms of financial loss, Action Fraud reports a total of £2.2bn lost by victims of fraud (including the 14% of fraud offences not cyber-enabled), with £99.3m lost by businesses to mandate fraud and over £220m lost by business and individuals to cheque, plastic card and online bank account fraud.² A further £40m was lost to cyber-dependent crimes, with £19m of this resulting from the victim’s social media or email accounts being hacked. Overall, 3% of those who reported a crime to Action Fraud judged themselves as having experienced a significant or severe negative impact as a result of being victimised (City of London Police, 2019c; City of London Police, 2019d).

For Hampshire and the Isle of Wight, the statistics are equally concerning, with 82% of just over 14,700 fraud related crimes being cyber-enabled, amounting to losses of almost £29m.

¹ Cyber-enabled frauds are defined by the National Fraud Intelligence Bureau as those “where the crime has an element of cyber but the technology was used to facilitate the crime, rather than commit the crime itself.” Cyber-dependent crimes are crimes that can only be committed using a computer, for example computer viruses, malware and spyware, denial of service attacks and hacking (City of London Police, 2016).
² Mandate fraud involves the victim being fraudulently persuaded to change a direct debit, standing order or bank transfer in favour of the criminal.
The 740 cyber-dependent crimes reported increased those losses by a further £821,000 (City of London Police, 2019a; City of London Police, 2019b).

In contrast to the Action Fraud statistics, experimental data collated by the Crime Survey for England and Wales (CSEW) estimates that to the year ending December 2018, there were 3.6 million occurrences of fraud nationwide, of which 63% were cyber related. The most common offences were bank and credit card fraud (67%) and consumer and retail fraud (28%). Around 18% of victims received no or only partial reimbursement. The CSEW also recorded 976,000 computer misuse incidents, of which 52% relate to hacking or other unauthorised access and 48% to computer viruses, with 33% of computer virus victims receiving no or only partial reimbursement (Office for National Statistics, 2019a).

When the CSEW figures are compared to the Action Fraud figures (which also include crimes against organisations as well as individuals) it suggests a significant number of incidents are going unreported to the police. Despite the size of the problem, progress is also being made in relation to protecting against cybercrime. For example, the 2018 CSEW statistics for computer misuse are down from 1.9m in 2016 with much of this improvement relating to reductions in reported computer viruses (down from 1.275m in 2016 to 471,000 in 2018) (Office for National Statistics, 2019b).

Certain demographics may be particularly vulnerable to specific types of cybercrime. For example, young people may be at greater risk of victimisation because of their high technical literacy, resulting in more frequent use of the internet, combined with a lack of appreciation for the capacity for criminal behaviour in others (Bolimos and Choo, 2017). One survey conducted in 2014 found that almost 18% of children aged 11-15 had experienced cyberbullying and, in the five years up until 2015/16, Childline saw an 88% increase in counselling sessions relating to online bullying (Brooks, Chester, Klemera and Magnusson, 2017; NSPCC, 2016).

In relation to older people, some studies have indicated this group may be less likely overall to become victims of cybercrime. For example, the 2017 Eurobarometer survey found that over-75-year-olds were the least likely age-group to be victimised in 8 out of 10 categories of cybercrime, although these statistics include those who never use the internet (European Union, 2017). However, other research suggests that older people may be particularly vulnerable to online fraud and, when they do become victims, are more likely to lose larger sums of money (Bolimos and Choo, 2017). A survey conducted by Age UK (2015) found that 53% of people aged 65+ believed they had been targeted online by fraudsters and while only 1 in 12 had responded to the scam, the charity estimated that up to half a million older people may have lost money to cybercrime.

In relation to organisations, small and medium businesses may be at particular risk of being targeted by cybercriminals due to a lack of expertise and resources and a perception that it is too costly to invest in appropriate IT security. This leads to a tendency to respond to cybercrime reactively instead of proactively. There is also a perceived lower risk for the

---

3 The CSEW records individuals’ experiences of crime regardless of whether the crime was reported and will therefore capture incidents not included within the Action Fraud statistics.
cybercriminal in targeting smaller organisations (Emm, 2013; Low, 2017; Paulsen, 2016; Renaud, 2016).

The 2019 Cybersecurity Breaches Survey found that 31% of micro and small businesses, and 60% of medium businesses had experienced breaches or attacks in the last 12 months. The mean annual costs for businesses that lost data or assets following a breach were £3650 for micro / small businesses and £9270 for medium businesses. For charities, 19% of low-income charities and 32% of medium income charities had experienced breaches or attacks in the last 12 months, with the average cost (across all charities including larger charities) for those losing data or assets being £9470 (DDCMS, 2019).

While the statistics show worrying levels of ongoing cybercrime victimisation, they do not reveal the full picture. Action Fraud, for example, does not accept reports in relation to cyberbullying or online child exploitation, and it is unclear how many incidents of cyber-dependent or cyber-enabled cybercrime victimisation go unreported, or even if some individuals are aware of having been victim to a cybercrime. In addition to data about the frequency of cybercrimes, many academic studies into factors surrounding cybercrime victimisation have been conducted. However, differences in the methodologies used can make it challenging to compare findings, which results in a fragmented picture, especially at a local level, and more work is needed to ascertain the true extent of cybercriminality.

2.3 Aim and Objectives

The project’s overall aim was to design, pilot and produce an implementation plan for a cybercrime awareness clinic, benefiting the local community and in particular groups vulnerable to cybercrime such as children and young people, older people and small to medium organisations, to meet the following needs:

- respond to the need to enhance our multi-stakeholder response to cyberthreats by becoming a forum for multi-stakeholder collaboration;
- uncover and map hidden crime to facilitate the police service’s understanding of the associated risks and types of victimisation within the community, enabling them to develop more appropriate and timely responses;
- provide a transferable model for the implementation of cybercrime awareness clinics in other parts of the country;
- educate key local stakeholders including the police, schools and businesses, through cyber-awareness seminars and workshops;

---

4 See, for example, Agustina (2015), Hernandez-Castro and Boiten (2014), Kerstens and Jansen (2016), Leukfeldt (2014) and Saridakis, Benson, Ezingeard and Tennakoon (2016).
5 A useful overview of some of the challenges pertaining to cybercrime victimisation methodology is provided by Hensen & Reyns (2016).
• increase hands-on practical opportunities for students by identifying related placements and linking those to graduate studies in cybercrime at the University of Portsmouth.

In order to meet the aim and objectives, the clinic operated three main strands of activity:

• Public engagement and advice – the clinic developed and delivered tailored advice on raising awareness of and building resilience to cybercrime for individuals and organisations through a variety of mediums (e.g. face to face, email, social media, presentations / seminars / workshops);

• Research – the clinic conducted research with children and young people, older people and small to medium organisations, as to their experiences of and concerns about cybercrime and how they would like to receive cybercrime awareness advice in the future.

• Finally, by building on the experiences and findings of the advice and research strands, the third strand of the project aimed to develop a transferable model for the implementation of cybercrime awareness clinics that could be rolled out in other regions.

This report summarises the clinic’s key activities in relation to the first two project strands: public engagement and research. More detailed findings from the clinic’s activities will be published in due course, in relevant journal articles.\(^6\)

---

\(^6\) If you would like further information in relation to the third strand of the project’s activities - the development of the transferable model for the implementation of cybercrime awareness clinics - please contact us, as we are able to offer advice, training and consultancy services: (Vasileios.Karagiannopoulos@port.ac.uk or cyber-awareness@port.ac.uk).
3. Summary of key findings and conclusions

“One of the most impressive aspects of the programme was its wide engagement with external stakeholders and experts in the field. This helped ensure that the Project would meet the needs of the local community in the best possible way.”

- Professor Donald Nicolson OBE
  Independent Project Reviewer

3.1 Public Engagement

3.1.1 Approach

In the early stages of the project, the clinic team focused on developing a comprehensive network of stakeholders including various relevant sections of Hampshire Constabulary, public and private sector organisations, charities and NGOs and schools and colleges. With their support, we were able to develop, promote and deliver a range of tailored cybercrime awareness sessions to local community groups, organisations and educational establishments. (Please see Appendix A for a detailed stakeholder map.) The range of engagement methods piloted included presentations, general talks and workshops, as well as one-to-one meetings, available both at the service user’s place of business or, introduced part-way into the pilot, by bookable appointment at the university.

The clinic team also developed a webpage, which incorporated a comprehensive list of cybercrime awareness resources, enabling service users to be signposted towards more specialist support if appropriate. Social media was used to share both original cybercrime awareness advice created by the team, for example memes, tweets and video blogs, as well as advice published by other reliable and verified sources.

3.1.2 Summary Findings

- General talks, presentations and workshops on cybercrime awareness for community groups and colleges were consistently popular and, once established, required minimal promotion as word of mouth and recommendations led to stakeholders approaching the clinic to request events;

- Engaging with schools was challenging, despite support from relevant partner agencies. It was very difficult for schools to find the time in their busy curriculums to host cybercrime awareness sessions, and there was a sense that schools felt they had received sufficient cybercrime awareness input and did not require more. See sections 3.2.2 and 3.2.3 for further discussion on this point;

- Engaging with small and medium organisations was also challenging, with attendance at events being irregular, despite promotional support from organisations
such as the local Chamber of Commerce and Federation of Small Businesses. The reasons for and implications of this are discussed further in sections 3.4.2 - 3.4.3. However, many events were well-attended, demonstrating that it was also a matter of context and organisation;

- One-to-one appointments with businesses were more popular when these took place at the business address, rather than at the university. See sections 3.4.2 - 3.4.3;

- Engagement online was variable, with Twitter and LinkedIn accounts proving effective platforms, whereas Vimeo (for uploading video blogs about cybercrime awareness) and Facebook were less successful;

- Generally, the clinic needed to be proactive in terms of reaching out to the public and undertaking public engagement activities. Passive tactics, such as bookable appointments at the university with members of the clinic team, were not popular with service users. Indicative feedback suggests that this was also because the times available were inconvenient or it was too intimidating for people to come to the university;

- Public engagement was challenging over the summer period for a number of reasons, including clinic staff taking leave, school / college holidays and community groups being on hiatus;

- As the research activities grew, especially towards the end of the project, it became more challenging to balance the time required for the Clinic’s research activities with public engagement commitments and some public engagement activities needed to be scaled back;

- The informal findings from the stakeholder engagement activity supported the more formal findings from the research activities;

- There was an initial lack of coordination with other cybercrime awareness initiatives in the local area, which had the potential to cause duplication of effort as well as ‘research / advice’ fatigue in the target population. This was mitigated by promoting collaboration between initiatives where possible;

- Evaluation of public engagement was a very challenging process, due to event formats and time constraints making it difficult always to get participants to complete feedback questionnaires.

3.1.3 Conclusions

- When offering one-to-one bookable appointments for members of the public that service users can attend away from their place of business, it is recommended to hold these in a neutral space ‘off-campus’ if resources allow. This was not possible during the course of this project based on its existing resources;
If possible, identify a centralised forum locally, to enable coordination / collaboration with partners working on similar initiatives and avoid the negative effects of ‘advice/research’ fatigue among service users and potential research volunteers;

- Plan ahead with community group leaders / event coordinators to ensure time is available for completion of feedback questionnaires during public engagement sessions and arrange for future follow-ups to measure long-term progress and impact. It is advisable to factor a potentially low response rate into evaluation plans.

3.2 Research with Children and Young People

3.2.1 Approach

An online survey was developed in consultation with colleagues at Hampshire Constabulary, the Office of the Police and Crime Commissioner and local schools and colleges, consisting of a combination of Likert Scale and multiple-choice questions, with the option for respondents to provide additional context in a free text field if desired. The surveys were administered by the school or college on behalf of the research team.

Our clinic school survey has so far collected 251 responses from an age group between 11-13 years of age. Our college research has been conducted across two colleges in the region and we have collected 103 responses. From these, nine responses were excluded as they indicated that they were mature students beyond 25 years of age. The college sample is further expanded by an additional sample of 80 school respondents aged 16-18.

Some supplementary precursor research was also conducted with two additional schools in the Portsmouth area. The precursor questionnaire focused on year 7 and year 10 pupils, with a total number of 394 responses. The combined results from both surveys provide us with a significant amount of students in terms of revealing a snapshot of the major issues and concerns for young people between 11 and 25 years of age. The clinic team will continue to refine its results as more responses are provided from the pending cohorts of pupils and additional local schools taking part in the research as well as the public engagement activities.

3.2.2 Summary Findings

- Cybercrime victimisation is very common, even at a young age with a limited amount of internet activity;

---

7 The precursor survey was conducted by Dr Vasileios Karagiannopoulos, Institute of Criminal Justice Studies, University of Portsmouth and Mr Simon Marsden, School of Education and Childhood Studies, University of Portsmouth.
• Children and young people were reluctant to report incidents, such as cyberbullying, due to a perception they would be blamed or no effective action would be taken by their school or college;

• Sexting is generally normalised with young people aged 15+, particularly when taking place within relationships;

• It is inevitable that pupils, even at a young age, will view harmful content online. Many pupils reported having seen violence or pornography online, which was concerning but not unexpected. Furthermore, responses indicated a rising popularity of religious or political material advocating violence, or sites promoting self-harm and eating disorders, which poses additional concerns for the wellbeing and safety of young people.

• Platforms where children and young people may encounter cybercriminal behaviour change rapidly and can be quite ephemeral. This presents challenges not only to authorities, but also to schools and parents, as they try to assess and supervise young people’s use of social networks and gaming platforms. In many cases, parents and teachers may be totally unfamiliar with some of the platforms frequented by children, who may then transition to new platforms within the space of months;

• Internet and gaming addiction were identified as potential concerns that can eventually have an impact on school performance and lead to sleep deprivation. This concern was reinforced through discussions with school nurses during public engagement activities;

• Schools seemed to feel they had received an adequate amount of cyberawareness-related sessions aimed at pupils, both internally and from external stakeholders. In addition research-related requests contributed to the challenges of recruiting schools to participate in the research;

• Older pupils and college students demonstrated reduced trust in the knowledge and currency of the advice they felt they would receive from teachers and parents / carers;

• Trusted adults and teachers are the main sources of online safety advice and guidance for younger pupils, even when the advice they provide is considered obsolete. Taken in conjunction with the previous two points, this highlights the need to steer cyberawareness sessions towards parents/carers and teachers rather than young people themselves.

• Adoption of protective measures, such as installing antivirus software and reviewing social media privacy settings, was patchy although very few respondents did nothing at all to protect themselves;

• A worrying percentage of pupils and students did not think that posting threatening or racist messages online, or getting someone to join a political or religious group that advocates violence, was a criminal offence.
3.2.3 Conclusions

- Cybercrime awareness education needs to start from an early age and focus on personal awareness and responsibility;

- Stakeholders need to collaborate to identify ways in which victims can report cyber victimisation without incurring further repercussions;

- Cyberawareness messages need to focus on critical thinking and empowerment of young people to facilitate the rejection of extreme ideas such as violent radicalisation, self-harm challenges (such as Blue Whale) or “thinspiration” (pro-anorexia / bulimia online fora and groups);

- Sexting should be managed through awareness and empowerment, rather than prohibition, but also through a process of enabling pupils to take control of what information they are sharing online. In-depth discussions are required with relevant stakeholders, such as the police, technology firms and schools and pupil groups in order for more efficient responses to be found, potentially with the use of technology;

- Cyberawareness education for teachers and parents should include messages around the constantly changing platforms used by children and the need for parents to be responsible and informed users themselves;

- Cyberawareness education for both young people and teachers / parents should include information relating to internet and gaming addiction as part of a general online hygiene;

- Future cyberawareness initiatives for younger children should be aimed at teachers, parents and carers, as a feasible route towards communicating more relevant and updated messages to pupils; adoption of cyberawareness advice is based on the legitimacy of the advice, which in turn is based on the currency of the advice and its communication in inclusive and non-prohibitive language.

- For older pupils and students, stakeholders need to develop and support schemes to train young people to deliver advice on cybercrime to their peers. An example of this would be the Cyber Ambassadors scheme run by the Hampshire Office of the Police Commissioner, which needs to be expanded;\(^8\)

- Children and young people should be educated to perceive cybersecurity as a cluster of different actions that are mutually reinforcing, including the provision of practical workshops to demonstrate how such safeguards can be put in place and the potential impact of not taking security measures;

- Children and young people should be educated in critical evaluation skills to help tackle the negative influences of fake news, in particular content that would steer

\(^8\) More information about the Cyber Ambassadors scheme can be found here: https://www.hampshire-pcc.gov.uk/get-involved/youth-commission/campaigns/gofish/secondaryambassadors
them towards self-harming behaviours, abusive relationships or violent extremist initiatives;

- Safeguarding messages that portray young people as unaware of the risks and in need of adult supervision and protection go against a generally communicated message in our research that young people feel they know more than their parents and teachers, especially as they grow older. Efforts should shift from safeguarding rationales, which encourage a more passive perception of young people at risk, to increasing young people’s awareness, resilience and personal responsibility.

### 3.3 Research with Older People

#### 3.3.1 Approach

Research with older people (aged 60+) was conducted by means of focus groups and individual interviews, using questions developed in consultation with Hampshire Constabulary and Portsmouth City Council’s Adult Social Care team. A total of 15 individuals (3 focus groups and 3 individual interviews) took part, recruited via a range of methods including via the University of Portsmouth’s Ageing Network (UPAN), through community groups such as Portsmouth Pensioners’ Association and in social clubs organised by Portsmouth City Council.

#### 3.3.2 Summary Findings

- The formal findings from the focus groups and interviews were remarkably consistent with the informal messages emerging from the public engagement activities with older people;

- The majority of participants were regular internet users with access to multiple devices and engaging in a wide range of online activity. This may not necessarily be representative of this age group, as our recruitment would have excluded most non-internet users and low-internet users may have been less interested in taking part in our engagement or research;

- Participants tended to rely on family members and paid IT professionals for support using the internet, rather than seeking external advice from the charity or education sectors. This has potential implications for those without family close by or the financial means to employ an IT professional. However, many participants also identified members of their peer group as being a desired source of cybercrime awareness advice;

- There was confusion around cybercrime related terminology, such as phishing, vishing etc., but a good understanding of the nature of the scams behind the terms;

- Concerns related to being online were diverse and often very personal, but frequently rooted in a fear of technology or a fear of change;
• If requirements for improving password security were too onerous, participants tended to take no action and stick with historic, risky password practices. Participants were also reluctant to use password managers or multi-factor authentication, perceiving these options as being beyond their technical capabilities;

• The numbers of participants who had been victims of cybercrime was surprisingly high compared to the relevant literature. However, reporting was low with most participants advising only the relevant organisation, such as a bank or online shop, but not the police or Action Fraud. There was a general belief that the police had better things to do with their limited resources. The one participant who did report his experience to the police was not satisfied with the response he received. This reinforces the general impression that follow-up information after reporting was considered inadequate by victims that reported cybercrimes to the police or Action Fraud.

3.3.3 Conclusions

• Consider establishing schemes to train confident older internet users to involve them in the provision of cyberawareness support and advice to their less confident peers. These could be based on a similar model to the Cyber Ambassadors Scheme for children (see section 3.2.3). This will be even more beneficial for older users with no financial means to hire dedicated IT support or without any experienced family members from whom they can seek cyberawareness advice.

• Professionals working with older people, for example librarians and occupational therapists, should be trained to be able to provide basic cybercrime awareness advice, which could be during specific cyberawareness sessions or as part of other routine activities;

• Cyberawareness providers need to proactively reach out to the most vulnerable members of this age group, by going into rest homes, libraries and cafes, to ensure engagement can happen even with those who are more isolated and don’t attend community events;

• A pragmatic approach to password management is advisable. This approach should balance risk expectations and the need for password security with what older people may find manageable on a practical basis, thus mitigating the risk of taking no action at all due to finding the advice provided too complex;

• Older people may require practical support with setting up and using features such as password managers and multi-factor authentication. Developing dedicated supporting resources and reference materials for this population is important; especially materials they can take with them (handouts) and practical exercises to enable ‘learning by doing’;

• Cybercrime awareness sessions with older people should be followed up, where possible, with a further session in 3-6 months to consolidate learning and
compensate for the rapid technological developments and the fast-changing threat landscape.

- Cybercrime awareness should include education on options for reporting cybercrime victimisation and challenge the perception that reporting such crimes is a drain on police resources.

3.4 Research with Small and Medium Organisations

3.4.1 Approach

A set of interview questions aimed at managers of small (including micro) and medium organisations in the local community was developed with the assistance of Hampshire Constabulary. The clinic team interviewed in-depth eight SMOs based in the Portsmouth area, addressing their cybercrime awareness, practices and experiences. The majority of our sample was from smaller organisations.

The formal findings from the interviews were consistent with the informal messages emerging from the public engagement activities with small and medium organisations;

3.4.2 Summary Findings

- SMOs were broadly aware of the threat that cybercrime posed to them in the sense that they understood their organisations could be targeted. However, they were generally unaware of the prevalence of cybercrime and were often uncertain about what constitutes a cybercrime, leading to insufficient preventative measures being taken;

- There was a satisfactory level of awareness of the significance of personal data such as customer information and the possibility of reputational damage as a result of a breach;

- There was little consideration given to the potential cybersecurity risks relating to employees and volunteers leaving the organisation;

- There was confusion about the correct steps to take in response to a breach, including whether breaches should be reported and to whom;

- While SMOs highlighted the need for cybersecurity training, there was poor awareness of how to obtain this and poor take up when support was available potentially due to time constraints and lack of staff to cover for those absent in training;

- Resources and management of various costs associated with cybersecurity was a crucial consideration, with concerns about this meaning cybersecurity is often not prioritised by SMOs;

- SMOs with more robust financial backgrounds were able to employ external cybersecurity support, whereas others with more limited resources relied on
themselves or non-specialist employees whom they consider to be tech-savvy for dealing with information management and security;

- There was a lack of understanding of the dynamic nature of cybercrime regarding how threats are constantly evolving, leading to a potential reliance on outdated training or information;

- There was a gap between SMOs awareness of certain risks, for example the need for securely-protected passwords which was clearly acknowledged, and actions actually taken to address the risk, e.g. passwords sometimes being physically written down;

- There is a lack of consistent messages received by SMOs about how to protect and mitigate against cybercrime. There was little to no awareness of national campaigns and initiatives or of government organisations especially set up to deliver practical guidance, such as the National Cyber Security Centre. Primarily SMOs seem to deal with cyber issues in-house or outsource them to security companies and often are not looking to engage with such content themselves or do not know how and where to obtain authorised support and information.

- There was greater concern over adhering to legislation than protecting against cybercrimes, although SMOs have started making the connection between their General Data Protection Regulation (GDPR) obligations and cybercrime prevention;

- Some SMOs were aware of cybercrime attempts against their organisations but were confident they were adequately prepared and able to avoid them. Very few of the interviewed SMOs divulged having been victims of cybercrime to their knowledge. Types of cybercrime that had been experienced included Denial of Service attacks (DDOS), stalking, website hacking, fraud, identity theft and theft of intellectual property;

- In terms of reporting cybercrime, SMOs felt they might not be taken seriously, would be wasting police time, or police do not have the resources to deal with cybercrime. Some SMOs were more inclined to report cybercrime to their bank, particularly if they felt they could rectify the situation and be reimbursed, and would not therefore also report to the police or Action Fraud.

- SMOs did not perceive Action Fraud to be a useful reporting mechanism for cybercrime, reinforcing the informal findings of the clinic’s public engagement activity where a general view was that the Action Fraud website was impractical and there was not much faith complaints would be followed through;

- When dealing with a cybersecurity incident, some SMOs preferred to seek the support of IT specialists to whom they have outsourced their IT practices, and would not progress further, if it could be dealt with in-house.
3.4.3 Conclusions

- Cybersecurity awareness initiatives should develop SMOs’ understanding of what constitutes cybercrime, which of their assets might be appealing to cybercriminals and what forms of behaviour relate to specific offences in order to identify and recognise cyber threats;

- Cybersecurity needs to be fully considered as part of the initial process of setting up an SMO, with relevant advice routinely included in the information available to those starting new businesses or other organisations;

- Advice should be tailored to meet SMOs’ needs, including organisational goals; and provided in situations and locations convenient to them, such as their places of business. Trusted networks can also be drawn on to assist in emphasising the need to engage with cybersecurity;

- Cyberawareness sessions for SMOs should include the development of risk scenarios to help test the efficiency of organisations’ current policies and practices;

- A ‘little and often’ approach may be a much more realistic expectation for improvements than an expectation that SMOs will go from no policy and minimal practices to a robust system within a short space of time;

- SMOs' interest in complying with the GDPR could be developed as a driver to encourage better engagement with cyberawareness training and cybersecurity standards overall, by emphasising the link between information security and GDPR compliance;

- In order to enable SMOs to communicate their experiences of cybercrime more effectively, there is a need to improve reporting processes, along with support for keeping victims informed of the progress of investigations;

- Cybercrime awareness initiatives for SMOs should aim to improve access processes and become more inclusive through multi-stakeholder collaboration in order to reach less informed / engaged, and therefore, more vulnerable SMOs.
4. Next Steps and Overall Conclusions

"An excellent project which provides excellent value for money in helping to potentially reduce cybercrime and thus save police time and resources in the long-run."

- Professor Donald Nicolson OBE
  Independent Project Reviewer

4.1 Next Steps

The project has come to the end of its initial pilot phase and this report reflects all the work that has taken place in the past two years. The clinic team is satisfied that our main goals have been achieved and even surpassed. We are proud to have created a very robust network of stakeholders, to have conducted research with all the populations that we were planning to work with and to have created a transferable model detailing how the clinic operated, what challenges it faced and what we can learn for the future. We are delighted to say that another major goal has been achieved, which was the extension of the life of the project. The clinic has not only secured more funding from sources at a national and international (EU) level, but has become an intrinsic part of a new, successful course (BSc in Criminology and Cybercrime), thus generating internal university investment and contributing to student learning and employability.

All of the above will ensure the clinic can continue to operate and offer support and guidance to the local community and beyond for the coming years. The clinic will expand its mission to communities and vulnerable populations beyond its current remit and train students to become cyberaware professionals with valuable transferable skills and great professional experience. Finally, the clinic will continue to work with Hampshire Constabulary in developing and refining cybercrime prevent and protect practices and engage in mutually beneficial research in the wider area of cybercrime and cybersecurity. Further information about the Cybercrime Awareness Clinic’s future plans is available on our website or by request to the clinic team.

If you would like advice or training on how to set up your own cybercrime awareness initiative, please contact the clinic team (Vasileios.Karagiannopoulos@port.ac.uk or cyber-awareness@port.ac.uk).

4.2 Conclusion

This report is only the beginning in terms of reporting on the first pilot phase of the Clinic, with research papers and conference presentations due to follow in the coming months. Our ultimate goal is to reinforce the message that increasing cyberawareness and building resilience to cyberthreats is crucial to citizens’ everyday well-being as well as our economic
sustainability. It is important to realise that there is no perfect security and also that there is a need for concerted collaboration from a range of stakeholders in order to keep up to date with new developments and prevent cybercrime victimisation. Technology is constantly changing and thus developing a consistent and regular programme of providing current advice, offering a dedicated space where support services and guidance can be found and following up on citizens who have been victimised are crucial elements that all stakeholders involved in cybercrime prevention need to consider. Becoming more secure online and having a “healthier” virtual presence is a task that requires grassroots, multi-faceted effort and therefore, understandable and realistic information developed through collaborative processes with the community is key. Building such a bottom-up network has been an intrinsic element of this project from its inception and will continue to be in all its future work. It is our hope that our example will inspire similar initiatives in order to create a national grassroots cyberawareness network that can work on a local, regional and national level in order to provide training, inform policing initiatives and even shape governmental policy on issues of online harms and risks.
Appendix A - Stakeholder Map
Appendix B - References


Contact Information

Clinic Team
Dr Vasileios Karagiannopoulos - Director of the Cybercrime Awareness Clinic
Dr Lisa Sugiura - Deputy Director of the Cybercrime Awareness Clinic
Dr Annie Kirby - Research Associate, Cybercrime Awareness Clinic

Email
cyber-awareness@port.ac.uk

Website
www.port.ac.uk/cyberclinic

Social Media
https://twitter.com/UoP_CyberAware
https://www.linkedin.com/in/cyberclinic/
https://www.facebook.com/UoPCyberAware/