



**UNIVERSITY OF
PORTSMOUTH**

Victims of Computer Misuse

Main Findings

April 2020

**Professor Mark Button, Dr Lisa
Sugiura, Dean Blackburn, Dr Richard
Kapend, Dr David Shepherd and Dr
Victoria Wang**

Contents

Table of Acronyms	5
Executive Summary.....	6
Introduction	6
Methods and Profile of Victims	6
Perception of Computer Misuse Crime	7
Impact of Computer Misuse Crime.....	7
Financial	8
Disruption.....	9
Psychological and emotional impacts.....	9
Health impacts	9
Damage to reputation.....	9
Violation of the digital self.....	9
Loss of digital possessions.....	9
Falling Victim.....	9
Security behaviours.....	9
Victims’ response to victimisation	10
Reporting Computer Misuse Crime	10
Reasons for low reporting.....	10
Reporting experience.....	10
Advice and support received	11
Victims Needs	12
Conclusions and Recommendations	12
1. Introduction	16
2. What is Computer Misuse Crime?	16
Defining computer misuse crime	16
The extent of computer misuse crime.....	19
3. Methods and Profile of Victims	22
Methods.....	22
Profile of victims	23
Caveats.....	24
4. Victims’ Views on the Recognition and Perceptions of Computer Misuse Crime	25
5. Impact of Computer Misuse Crime.....	28
Financial	30

Disruption	31
Anger	32
Anxiety	32
Stress.....	33
Embarrassment and shame	34
Isolation	34
Damage to reputation.....	35
Negative changes in behaviour.....	35
Violation of digital self	36
Loss of digital possessions	37
Health Impacts	38
Suicidal thoughts/actions.....	39
SME/O	39
Financial	39
Disruption.....	40
Reputational damage.....	41
No significant impact	42
6. Falling Victim.....	42
The weak point.....	42
Victims with poor security habits	43
Passwords	43
Anti-virus.....	43
Risky behaviours	44
Lack of engagement with security standards for SMEs	44
Victims with good security habits	45
Victims' response to victimisation	45
Change in security behaviours	46
7. Reporting Computer Misuse Crime	56
Reasons for low reporting.....	56
Status of computer misuse related crime.....	56
There was no financial loss	56
Assumption non-police/Action Fraud initial reporting body would pass on.....	57
Reputation and experience of Action Fraud.....	57
The police are unlikely to do anything because they are too busy	58
Wrongly advised it was not a crime.....	58
Never heard of Action Fraud.....	59

Embarrassment and fear of the consequences of reporting	59
Other factors discouraging reporting to the police/Action Fraud	60
Other websites where CMC is reported	60
Action Fraud website	60
Police reporting websites.....	61
Reporting Experience of those Reporting to Bodies other than Police/Action Fraud.....	61
Experience of Victims whose cases were reported to the Police and/or Action Fraud	62
Reporting experience of those reporting to the police	64
Experience of those Reporting to Action Fraud.....	65
8. The Response of the Police/Action Fraud.....	68
Disappointment at Action Fraud classification	70
Frustration at perceived lack of action	71
Lack of any response.....	71
Response to say no further action	71
Lack of information on progress of the case	71
Advice and support received from police/Action Fraud.....	72
Information/advice from Action Fraud.....	72
Awareness of sources for advice/support to prevent victimisation.....	73
Visit or contact from the police to take a statement or provide support	76
Experience of police investigation	78
Survey victims' views overall on Action Fraud, the police and other organisations compared	81
9. Victims' Needs.....	83
Information about the case and what happened.....	84
Technical support.....	85
Offenders brought to justice.....	87
Reassurance	88
10. Conclusion and Recommendations.....	88
References	92
Appendices.....	94
Appendix 1. List of interview victims and type of offence.....	94
Appendix 2. Demographics of survey and interview victims.....	97
Appendix 3. Non-police reporting websites	100
Appendix 4. Action Fraud Reporting Website	101
Appendix 5. Police Reporting Websites.....	102

Table of Acronyms

CMC – Computer Misuse Crime

DDoS – Distributed Denial of Service

ECVCU – Economic Crime Victim Care Unit

CSEW – Crime Survey for England and Wales

HMICFRS – Her Majesty’s Inspectorate of Constabulary, Fire and Rescue Services

ICT – Information and Communications Technology

NCSC – National Cyber Security Centre

NFIB – National Fraud Intelligence Bureau

NPCC – National Police Chiefs’ Council

ONS – Office for National Statistics

SIA – Security Industry Authority

SME/O Small Medium Sized Enterprise/Organisation

2FA – Two Factor Authentication

Executive Summary

Introduction

In the Summer of 2018 researchers at the University of Portsmouth were commissioned by the Home Office and Her Majesty's Inspectorate of Constabulary, Fire and Rescue Services (HMICFRS) to research victims of computer misuse with the broad aims:

- To examine the nature and impact of computer misuse related crime on victims;
- To assess the support provided to such victims and identify better means to prevent such crime; and
- To examine the experiences and perceptions of those victims who have experienced a law enforcement response.

Computer misuse crime (CMC) covers the cyber-dependent crimes largely grouped under the 1990 Computer Misuse Act of hacking related offences, computer virus/malware/spyware related infections, denial of service attacks and ransomware.

The reform of the Crime Survey for England and Wales (CSEW) with the addition of questions on computer misuse victimisation has exposed large number of victims: 470,000 of computer viruses and 500,000 victims of unauthorised access to personal information in the year ending December 2018 – which accounts for 9% of all CSEW crime (ONS, 2019a and b). The Cyber Security Breaches Surveys, found relating to SME businesses that large numbers have experienced a cyber security breach in the previous year at 60% of medium sized and 40% of small (Finnerty et al., 2019).

Very small numbers of incidents are recorded by Action Fraud with 23,683 in 2018 illustrating significant under-reporting and attrition.

Methods and Profile of Victims

To conduct the research a literature review was completed, 7 stakeholder interviews, 52 interviews (38 individual and 14 SME/O) with victims and via 252 responses by individual victims to an online survey administered by Qualtrics were secured.

- The majority of victims secured via the survey and interviews had experienced some form of hacking at 62% of the survey and 34 of the 52 victims interviewed.
- 29% of the survey victims had experienced a computer virus or equivalent and 7 of the 52 victims interviewed.
- 8% of the survey victims were ransomware victims and 7 of the 52 victims interviewed.
- 1% of the survey victims had experienced a denial of service attack, with 2 of the 52 victims.
- Of the 52 victims there were also one who experienced multiple attacks and 1 who was the victim of harassment (although recorded as hacking).
- Of the 52 interview victims only 4 had secured a response that resulted in a criminal justice sanction for the offender.
- Only 13 received some form of police response such as a telephone call, visit or communication concerning an investigation.

- 18 victims reported and received no further action, with a further 5 who attempted to report, but were either denied the opportunity or there was no further action. 12 did not report to the police or Action Fraud.

It is important to note some caveats relating to the methods used. The online survey is not representative of wider population of computer misuse victims; interviews were purposive and designed to get a spread of different types of respondents; and interview recall wasn't always very good and some victims struggled to understand what type of offence had actually occurred.

Some of the victims for this research were supplied via the National Fraud Intelligence Bureau and the categories victims were often recorded under were not always accurate. For example there was one victim of spam mail classed as a hacking victim, a victim of hacking classified as ransomware and a victim of a phishing attempt listed as a hacking victim.

Perception of Computer Misuse Crime

Both the majority of survey and interview victims rated CMC as either equivalent or more serious than traditional crimes such as burglary. On a scale of 1-20, with the latter the most serious survey victims rated burglary at 9.48, which compared to 8.26 for hacking for thrill, 8.98 for hacking to view personal information, 9.40 for sending a virus, 10.3 for hacking for fraud, 11.06 for sending ransomware and the most highly rated was 11.08 for hacking for voyeurism. The interviews did reveal a small minority who rated CMC a lesser crime.

Impact of Computer Misuse Crime

Both the survey and interviews with victims highlighted a wide variety of impacts that have been noted with other types of crime victim that included broadly: financial, psychological and emotional, health related, reputational as well as some new types of impact specific to these types of crime. The full report contains many actual quotes from victims, with their pseudonyms and the following box contains a small snapshot of quotes to illustrate victims' views.

The Impact on Victims in their own Words (Many more quotes in report)

...so they left me with nothing, and then our mortgage was due to go out and other payments and nothing would have... And I was scared of all the bank charges and that, so I had to borrow some cash. Claire [Hacking, Individual].

...knowing that I couldn't take any money out of the bank because there was nothing left was a bit shattering. Sarah. [Hacking, Individual].

I was frightened it was going to happen again. Yes. I was frightened that whoever had done that would know we were vulnerable and probably easy access and might find another way in". Kathy. [Hacking, SME]

God. On the Saturday and Sunday, that was probably about six, seven hours, just for the eBay and PayPal. Facebook was just...that was at least six hours on the day, speaking to Action Fraud and the police. And going on and off and trying to do stuff. And then ongoing messages to them. So easily...I'd say 32 hours, I'd say. Catherine [Hacking, Individual].

It's massive, the disruption in fact is massive. Rachael. [Denial of Service Attack, Individual].

...he put me through hell for a few months, and he invaded my personal world, and tried to take away my future and my kids' future, that's the way I saw it. Sophie. [Hacking, Individual]

Yeah I think for a couple of days I just couldn't stop crying and I felt so low, but after that, I think it did turn more to anger and wanting to fight to get my money back... Claire. [Hacking, Individual].

The other impact of course is a feeling of anger, I suppose, that someone would put you through such inconvenience in an attempt to extort money from you; so mostly it was financial. I didn't need any counselling. I mean it was just bloody annoying because when you've got work to do you want to get on, and some little oik has caused you to lose half a day's work. Steve [Ransomware, SME].

Oh, very stressful. I couldn't work. I didn't have time off work, I just sat at my desk and stressed, not getting work done. Alex. [Hacking, Individual].

It is stressful, it is frightening in lots of ways. And it's very distressing that something you could work on for two years, can just, in a heartbeat, disappear...It had never occurred to me that something you put on the internet, doesn't automatically stay there forever. Sabrina. [Hacking, SME]

Yeah. The doctor said I couldn't cope with what was going on because my mind was racing, I didn't trust anybody, I was going very withdrawn and literally within three months he doubled the dose and that's stabilised me. Leo. [Hacking, individual].

...it's going to sound really melodramatic, but at times it was life-threatening to me...anything could happen...and I would be a couple of times sat on the bridge wanting to throw myself off a bridge. Wayne. [Harassment, individual].

...they [the police] really underestimate the impact on a human being, you know. When it reaches the point where you, as I said earlier, you feel like you've been physically assaulted, then it should be treated as assault of some sort. Patricia [Multiple, individual].

I felt powerless, angry, violated in a way, very angry and angry because nobody would listen to it, 'cause I kind of put my trust in the police, thinking that I'd just been kind of dismissed in a way, just another domestic situation.. Husky. [Hacking, Individual]

I felt raped, you know, that somebody was watching me, so I was like I'm not using that laptop. Kathy. [Hacking, SME].

Financial

The survey victims experienced financial net losses ranging from £2 to £10,000, with a mean of £657 and median of £250. Many victims experience no financial loss at all. Some do not experience a direct financial loss from the crime, but experience costs in dealing with the consequences of the crime, such as purchasing anti-virus software, securing technical support etc.

Some SME/Os experienced substantial costs in dealing with the impact of CMC. In one case an SME incurred over £80,000 in costs dealing with the consequences of the incident. Another lost £40,000 and 70% of their customers as a result of a hacking attack.

Disruption

Many victims experience disruption as a result of a CMC. This can involve loss of access to services (such as banking, Facebook etc) or devices, time spent trying to deal with the situation and reporting it to relevant bodies.

Some SME/Os experienced major disruption in their ability to trade or offer services. Some organisations experiencing ransomware attacks lost all their computer files and were never able to recover them all, some lost access for short periods causing interference in operations for only short periods.

Psychological and emotional impacts

Many victims noted psychological impacts such as anger, anxiety, fear, isolation and embarrassment. According to the survey those noting any impact (great or fair amount): 75% noted stress, 70% anxiety, 52% fear, 51% embarrassment/shame/self-blame, 48% anger and 43% isolation.

Health impacts

Some victims reported the incidents had impacts on their physical or mental health. According to the survey those noting any impact (great or fair amount): 53% noted difficulty sleeping, 45% panic or anxiety related illness, 43% depression, 42% stress related illness and 38% change in appetite/weight loss/weight gain. A further 23% reported self-harm and 20% suicidal thoughts.

Damage to reputation

Some CMC can lead to damage to reputation. For example one victim interviewed experienced details of a past rape being exposed (among many other incidents) that damaged her reputation. Another victim almost lost a job offer, as a result of a hacking by her then current employer, which damaged her status with the prospective new employer.

For SME/Os reputation is often very important. Several enterprises reported probable loss of business as a result of the incident they experienced.

Violation of the digital self

Several victims interviewed described many of their digital devices and accounts as extensions of their physical selves and compared the attacks to acts of violation and in some cases even rape.

Loss of digital possessions

Some victims lamented the loss of digital possessions which were or were probably irretrievable as a result of the attacks such as photographs held in accounts, personal documents or email accounts.

Falling Victim

The interviews and the survey provided a great deal of information on the security behaviours before and after the incident.

Security behaviours

The interviews revealed a wide range of reasons as to why they had fallen victim to the crime. There were also some who had no idea how they had fallen victim.

Several victims described 'weak point' moments where they described what they considered generally strong resilience, but because of the circumstances of a particular time they had fallen victim to CMC. These included being in a rush, focus on specific task or wider personal issues. These were often then able to be exploited by good social engineering by the criminals.

Some victims reported poor security habits such as poor passwords, using the same passwords and easily guessable passwords, such as family names.

Several victims reported to using either no anti-virus, free versions or not updating it.

Risky behaviours were admitted by some victims as a probable cause of their incident, such as visiting unlawful sites to watch pirated movies.

Most of the SME/O victims had no knowledge of cyber security standards either before or after the incidents.

There were also victims both individual and SME/O who reported excellent security knowledge and application, but who still became victims.

Victims' response to victimisation

Both the survey and interviews found that there was generally limited changes in behaviour as a result of victimisation and that for many victims security behaviours were not strong.

The survey found there was a small increase in use of device passcodes, software updates, data back-ups and reporting; and a decrease in the use of device and website password managers. But there was no significant change in approach to protective authentication through strong passwords and 2FA for email accounts.

It also found the experience of harm is unlikely to lead to a significant increase in protective behaviours, with only a minority of persons more cautious and the majority not changing their behaviour.

Reporting Computer Misuse Crime

The research discovered a variety of findings on the reasons for non-reporting of CMC and the experience of those who do try to report.

Reasons for low reporting

There were many factors that contributed towards low reporting. These included:

- Some victims not considering such incidents as crimes;
- No financial loss occurring;
- Reputation and/or past experience of Action Fraud as poor;
- Victims wrongly advised by police/Action Fraud their report was not a crime;
- Victims never heard of Action Fraud; and
- Embarrassment or fear of consequences of reporting.

The research also found other service providers where victims often report first, such as Google, Facebook, banks etc do not always clearly suggest reporting such incidents to Action Fraud. Police websites were not always clear either on where to report such cybercrime and the Action Fraud website was more focused upon fraud than CMC.

Reporting experience

Some victims of CMC, particularly hacking victims, start with the relevant provider of the service where the hack has occurred to report, such as banks, Facebook, Gmail etc. For some victims this is the end of the reporting process, for others it is followed by a report to the police or Action Fraud. The survey and interview data generally illustrated a positive experience with such providers, particularly the

banks. However, there were some victims which highlighted challenges with speaking to and securing action from some providers of services via the internet.

Regarding reporting to the police and Action Fraud victims had made use of both websites, the telephone and reported in person. Those reporting to the police were generally unaware of Action Fraud and some just wanted to report to the police.

Regarding the police a significant number who reported to the police did so via 999 (36% of police reports). For both the police and Action Fraud the general satisfaction with the reporting experience was positive with just over 2/3 strongly or tending to agree their reporting experience were positive. Overall, however, this was slightly lower than other organisations that are reported to (banks, Facebook etc). There were, however, some negative areas where there was room for improvement in the services.

Some victims struggled to secure police acceptance of their case when there was clear evidence of a crime. Husky (an individual hacking victim) was wrongly advised her estranged husband hacking and monitoring her laptop was not a crime because they still lived together. Sam (an individual hacking victim) was wrongly advised the hacking of her webcam was not a crime. In another case Alex (an individual hacking victim) started with the police, was referred to Action Fraud, who then referred him back to the police. Where cases are complex involving offending over multiple forces there was also evidence of mixed responses.

The telephone reporting experience of Action Fraud was generally positive for the victims. For the website it was more mixed, although most of the victims interviewed reported to Action Fraud before the subsequent changes to the Action Fraud website reporting pages.

There was frustration among victims at the perceived or actual lack of action. Some victims had reported to Action Fraud and heard nothing. Some had heard news from Action Fraud, but this was to say there would be no further action, which was disappointing to them. Some victims claimed they had received no information on how the case had progressed.

It is also important to note there were also a small number of victims who were also very happy with their response from the police, Action Fraud etc; even in some cases where there was no investigation or no identification of the offender.

[Advice and support received](#)

The interview victims who reported generally did not receive extensive support from the police/Action Fraud. Other than letters, few recalled any substantive support to better equip them to prevent future incidents. Website links on letters were not always followed up by victims or even recalled by some. The websites that offer advice and support generally had low recognition among victims, both before and after the incident.

Among the victims interviewed a small number received a telephone call from the police and some a visit. Most, however, did not receive this, with a very small number receiving no response and some just a letter/email with no further follow up or updates on their case. SME victims of Ransomware were the most likely to receive a visit, but in most cases there was little the police could do.

Very few victims experienced a police investigation and even less a successful investigation. Of the 52 victims interviewed only 4 resulted in a conviction/caution for the offender(s) and 3 of these related to NCA cases.

Victims Needs

The survey identified immediate support such as where to go to, who to talk to as the highest ranking need (82% rated very or fairly important), followed by technical support (76.2%), information support (74.6%), emotional support (64%) and financial support (63.5%) as the five highest.

The interviews highlighted some of these. Many victims did not know what had happened and wanted to know what had occurred to them and to find out what the authorities were doing.

Technical support was a significant need among many victims and particularly some SMEs. For many of these the CMC caused disruption which affected the business/organisation and to return to normal required expert help not in the organisation. For example ransomware victims wanted support in accessing lost files and cleaning computers. The immediate point of the incident was when many victims wanted technical support. Several victims wanted to be sure their devices were clean and wanted external reassurance to achieve this. Technical advice to better protect for the future was also wanted.

Some victims were unsure where to secure such technical advice and relied on friends/family's recommendations or established brands such as PC World.

Several victims wanted justice and for the perpetrators to be brought to justice.

Some victims just wanted reassurance to know they were no longer at risk from attack and that the incident had passed.

Conclusions and Recommendations

This research has provided some important new data on victims of CMC. First it has shown that most victims regard CMC as an equivalent crime to traditional crimes like burglary, with some considering it more serious, with a small minority regarding it as a lesser crime. The research demonstrated victims experience many of the impacts that other crime victims experience, with some overlap with fraud. There were also some victims who suffered severe impacts, as well as some noting very small impacts and regarding it as little more than disruption.

The research explored how victims felt victim and showed in some cases they were tricked by sophisticated social engineering, some exhibited poor security behaviours putting them at greater risk, but some also had very good behaviours but still fell victim. The report explored the changes in behaviour as a result of victimisation and it showed in general there were not major changes. The reasons victims did not report were examined and then the experiences of those that did. The response of the police and Action Fraud, where there was a response was also explored. The research ended by considering what the victims wanted.

The findings from this research led the authors to make the following recommendations, which fall under the following categories: improving reporting, improving victim support and advice, increasing resources for tackling computer misuse.

Improving reporting

The experience of the researchers dealing with victims and trying to understand their interpretations of what happened illustrated the challenges of definition. This was highlighted further with data supplied by the NFIB, which showed there had been misclassification of victims, not just among web reporters. The research was conducted with data drawn before changes to the online reporting system and better quality checks were introduced. Many of these issues may therefore have already been

addressed. However, it is essential that those reporting cybercrimes are properly classified for both measurement, investigation and response issues.

Recommendation 1. The new systems for reporting, classifying and ensuring the quality of decisions undertaken by Action Fraud and National Fraud Intelligence Bureau (NFIB) should be regularly monitored and evaluated to ensure the classification of CMC reports for both telephone and web reporting are being classified accurately [Directed at Action Fraud/NFIB].

The central challenge of the name Action Fraud is for many victims this does not sound like a body cybercrime should be reported to, particularly when it does not involve fraud. Another challenge to reporting CMC (and fraud) is the name Action Fraud and the association of the word 'Action' with investigation and response, rather than reporting. Some victims actually think it is a special fraud investigation squad, which implies there will be an investigation by Action Fraud. For these reasons the researchers think the name should be changed.

Recommendation 2. Action Fraud should be renamed the 'National Fraud and Cybercrime Reporting Centre' [Directed at Home Office, City of London Police].

This report identified a number of barriers to individuals reporting CMC offences. There are a number of recommendations below which aided with a focused communication strategy could enhance reporting:

Recommendation 3. Greater prominence should be made of CMC offences on the Action Fraud website [Directed at Action Fraud].

Recommendation 4. All police reporting websites should be reviewed to assess information provided on reporting CMC and where there are gaps advised to more clearly indicate how cybercrime can be reported with relevant links provided [Directed to Home Office and all police forces].

Recommendations 5. The NCSC should work with key bodies such as Action Fraud, Getsafeonline; relevant service providers, such as banks, social networking sites, email providers etc who receive cybercrime reports, to provide a common set of words and website links to be placed upon their website to encourage them to report as crime [Directed to NCSC, Action Fraud and relevant website providers].

There was also evidence of some staff who might receive or advise on reports did not grasp the legislation relating to CMC, particularly related to non-financial related crime such as harassment, voyeurism and domestic disputes where the research found examples of victims being wrongly advised their case was not a crime. The authors therefore suggest that all relevant police staff and Action Fraud staff should receive training in CMC offences and where such training already occurs, it should be regularly reviewed to ensure those experiencing it clearly understand what constitutes this type of crime, the seriousness of it and options for victims:

Recommendation 6. All police officers, police staff and Action Fraud staff dealing with victims who may report crimes should be better trained in what constitutes CMC offences, particularly in relation to non-financial related cases such as voyeurism, harassment and domestic disputes; and the options for dealing with them [Directed to Home Office, College of Policing, Action Fraud].

Improving victim support and advice

The findings noted limited changes in behaviour by some victims from the survey and interviews. There were examples of victims who were hacked not improving their password security and

computer virus victims not engaging with anti-virus software. Some of the interview victims at the point of victimisation were clearly interested in cyber security, but were not offered appropriate tailored advice. This seemed to be a missed opportunity at the point of victimisation to enhance the resilience of the victim. The Economic Crime Victim Care Unit (ECVCU) pilot is an illustration of moves to more intensive support for this type of victim. This research has not evaluated the ECVCU and some of its activities would overlap with the following recommendation:

Recommendation 7. Tailored packages of advice/support (based on National Cyber Security Centre guidance/advice) relating to the specific type of incident should be supplied to the victim at the point of reporting and evaluation of this support should be undertaken regularly to improve it [Directed at Action Fraud and the NCSC].

Recommendation 8. Further research should be conducted to evaluate different approaches to targeting victims and the impact these have on behaviours and future victimisation [Directed at Home Office].

There was evidence of victims not receiving information on the progress of their case, which is contrary to the Victims Code. There was also considerable variation in the nature and extent of the responses victims received.

Recommendation 9. Action Fraud and the police should do more to ensure victims do receive timely information on what has occurred in relation to their case [Directed at the police and Action Fraud].

The Action Fraud website was the most recognised by victims, but the research team's views were that it was not necessarily the best at supplying information to victims on prevention, support etc of CMC related offences. Getsafeonline and the National Cyber Security Centre provided the best advice in the view of the research team, but were low down the recognition list of victims. Action Fraud could either develop new website or link in a more effective way to the better websites. It might also be prudent to conduct some research with victims to determine the most effective websites for offering advice.

Recommendation 10. Action Fraud, with the most recognised website offering advice, should work with the National Cyber Security Centre to ensure consistent and technically accurate advice on preventing and dealing with cybercrime is provided to victims. This should also be built upon research to determine the most effective websites for interesting and changing the behaviour of victims [Directed at Home Office, Action Fraud, National Cyber Security Centre].

Increasing resources for tackling computer misuse

The findings for this research found many victims who did not receive a police investigation or any other form of police interest. Some victims did not want any police support, but many did. There were also cases where victims thought they had clear leads on who the offenders were (although in reality those leads may have been weak), but nothing occurred. It is clear that many victims who want police support do not receive it. There are clearly not enough resources of the police dedicated to CMC and many of the resources that do exist are built upon short-term funding, with no guarantee they will continue (HMICFRS, 2019). The authors believe more resources should be dedicated to this crime, how much, however, is clearly a political decision when there are so many demands on the police.

Recommendation 11. The police should dedicate greater resources towards tackling CMC [Directed at the Government, Home Office and the police].

It is clear that even with more resources the police could not fill the gap in the support that victims want. Technical support was one of the main needs identified by victims and many of the demands that fall under this would not necessarily be something the police could or should provide, particularly in relation to SMEs. There is a challenge, however, of where to go to secure technical advice and who to trust. There are other examples in physical security of official schemes to indicate compliance with standards and that the operator is a legitimate supplier such as the Security Industry Authority's Approved Contractor Scheme and the police service's Secured by Design initiative. The National Cyber Security Centre has a variety of certification programmes, but these do not currently cover providers of cyber security services at the front line of victims. A scheme that provides a kite mark of approval and list of suppliers that could be provided to individual and SME victims would aid them in securing appropriate professional support.

Recommendation 12. The Government should encourage a scheme to recognise suppliers who are accredited to appropriate standards to provide cyber security technical services to individuals and SMEs, similar to schemes such as Secured by Design and the SIA's Approved Contractors Scheme. Victims could then be provided with links to a website which includes a list of relevant suppliers who have met those standards [Directed at the Home Office and National Cyber Security Centre and the NPCC].

1. Introduction

The reform of the Crime Survey England Wales (CSEW) to include questions relating to fraud and computer misuse crimes (CMC) has exposed the significant levels of victimisation among the general public, accounting for over 40% of crime. There is, however, relatively little research on these new crimes in comparison to the traditional volume crimes and with the computer misuse offences even less. This research project has explored the views and experiences of CMC victims. It is one of the first studies to offer a deep assessment of these victims using largely qualitative research.

The report will begin by exploring what is CMC, it will then briefly set out the methodology used. Given the new nature of these crimes and the gap in knowledge in their status among victims the report will then explore this, followed by the impact such crimes have on the victims. The report then explores how and why victimisation occurred and examines some of the behaviours. These sections provide clear context to the nature of CMC offences and how serious they are. This provides clear foundations to then explore why victims do not report, the experience of those that do and their views on the services they receive. The report then examines the needs of these victims and ends with a conclusion and list of all the recommendations made throughout the report.

This report has been produced alongside two other outputs. There is a literature review that was conducted at the start of the project in the Autumn of 2018. This has been updated as the project progressed and for this reason this report will only reference relevant literature where necessary. Readers interested in the broader literature should consult that output. Second there is an output of 52 case studies of the victims interviewed. This, in the victims' own words, provides a detailed explanation from the victim of what happened, their response (and the relevant bodies where there was one) and the impact. The report is best read alongside these other outputs from the project.

2. What is Computer Misuse Crime?

Defining computer misuse crime

Computer misuse crime can broadly be divided into two areas:

- the unauthorised access to a person's or organisation's computer or related device and/or online accounts (including by hacking); and
- the distribution of viruses and associated malware to disrupt or extort victims (ONS, 2018a).

The principal piece of legislation these offences fall under is the Computer Misuse Act 1990. This, however, does not restrict the offence to a 'computer' as it, 'can include any device using operating software accessible online, for example, games consoles, smart phones and smart TVs' (ONS, 2018b, p 2). The principal offences under this legislation are:

Hacking offences:

- Section 1: Unauthorised access to computer material
- Section 2: Unauthorised access with intent to commit or facilitate commission of further offences.

Computer virus offences:

- Section 3: Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.
- Section 3ZA: Unauthorised acts causing, or creating risk of, serious damage.
- Section 3A: Making, supplying or obtaining articles for use in offence under Section 1, 3 or 3ZA.

Action Fraud/National Fraud Intelligence Bureau (NFIB) provide some more detail on the types of crime under this category by distinguishing the following reporting categories (Under NFIB 50):

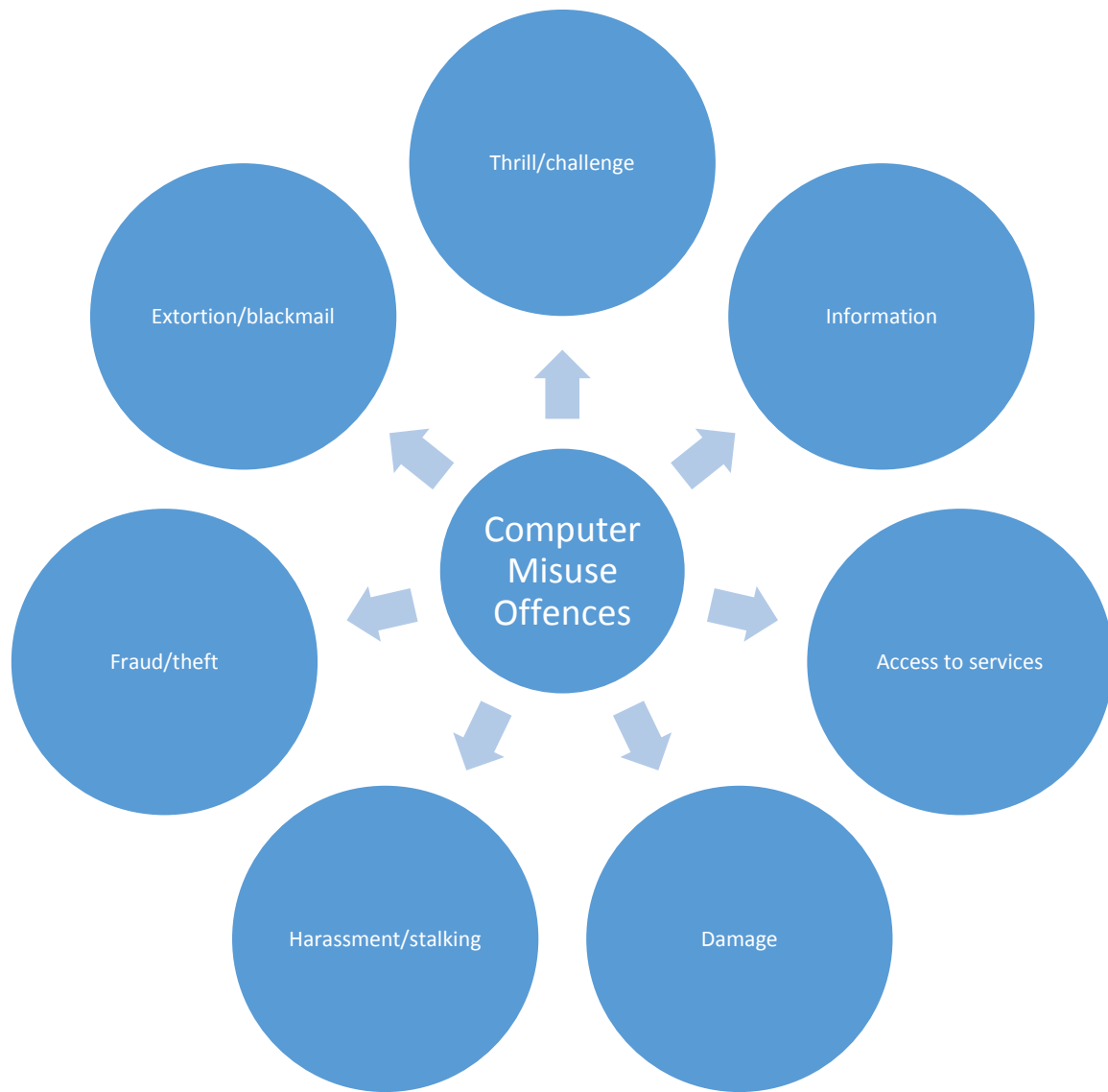
- Computer viruses/malware/Spyware (NFIB50A);
- Denial of service attack (NFIB51A);
- Denial of service attack (extortion) (NFIB51B);
- Hacking – server (NFIB52A);
- Hacking – personal (NFIB52B);
- Hacking – social media and email (NFIB52C);
- Hacking – pbx/dial through (NFIB52D); and
- Hacking – extortion (NFIB52E) (ONS, 2018b).

In the UK the distinction between *cyber-enabled* and *cyber-dependent* crime has become the most common means to distinguish a range of crimes (Furnell, 2002; Levi et al, 2015 also distinguish *cyber-assisted*). The former are crimes that do not require information communications technology (ICT) to commit them, but can be expanded by the use of such technology. For example a lottery fraud could be perpetrated by traditional mail, but also by e-mail. *Cyber-dependant* crimes, however, can only be perpetrated by ICT (ONS, 2018b). All computer misuse offences are cyber-dependent. However, as noted above, other means, not necessarily cyber-dependent, might be used to help facilitate the offence.

The nature of computer misuse, however, means that other offences also frequently combine with it. Offenders for instance might use phishing techniques to secure personal information to enable access to accounts (fraud by false representation) or corruption of persons with access to such information (bribery offences) and once they have secured that information, then access the accounts/computer (computer misuse) of the victims. When they have secured access they might find embarrassing information and use that to blackmail the individual (blackmail). They may then seek to clean the money they have extracted from the victim (money laundering). Thus one act of computer misuse might be part of a much wider range of offences. Most commonly, however, computer misuse offences are used to facilitate thefts and frauds, among other offences. As figure 2.1 below illustrates there are a variety of consequences/aims of using computer misuse related acts some of which might not be criminal, some criminal and some civil torts. Starting at 12 o'clock the CM offence might be the sole offence. A person hacks into another account for the thrill to see if they do it or to

check if their partner might be having an affair. They might hack into an account to use another person's services, such as Netflix or Facebook or to damage their reputation by defacing a profile or placing malware on a computer. At 7 o'clock on Figure 2.1 more serious offences begin to emerge where the CM offences are used to commit increasingly more critical offences such as harassment/stalking, fraud/theft and extortion/blackmail.

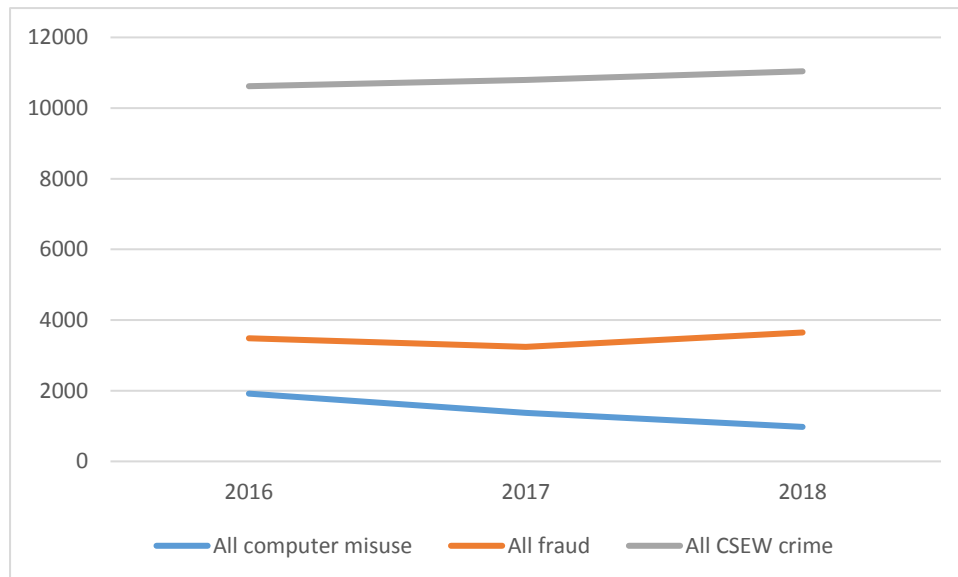
Figure 2.1. Computer misuse offences and their links to other behaviours/crimes



The extent of computer misuse crime

The most accurate measure of crimes against individuals is the Crime Survey for England and Wales. Statistics relating to computer misuse have only been gathered in the last few years. Figure 2.2 below shows the last three years of data for the years ending December 2016-2018:

Figure 2.2 CSEW computer misuse offences in comparison (000s)



ONS (2019a and 2019b)

The table shows a slight increase over the period for all CSEW crime and fraud, but a significant decline in computer misuse offences.¹ As the next Figure 2.3 shows, this has been caused by a significant reduction in computer viruses. It shows a reduction in computer viruses from just over 1.2 million in 2016 to 470,000 in 2018 (years ending December). Unauthorised access to personal information has also declined, but only from just over 640,000 to just over 500,000 (years ending December). Even with this decline, however, CMC account for around 9% of all crime.

The other measure for this crime are the number of computer misuse offences recorded by Action Fraud. These show a different trend with an increase of just under 14,000 offences recorded in 2015 to 23,683, an almost 70% increase. Part of this increase is likely to reflect increased awareness of Action Fraud and encouragement to report such crime. However, what is perhaps the most significant issue is the significant attrition with the numbers recorded representing a tiny percentage of the level of victimisation, with the experimental statistics of ONS (2017) showing only 6.4% of computer misuse offences the police becoming aware of or reported to Action Fraud. It must also be remembered the Action Fraud data also includes reports by organisations and therefore this non-reporting and recording is likely to be an even lower percentage.

¹ Caution should be taken when looking at the overall trends over time, given the short time series currently available. Although fraud and cyber estimates were introduced into the CSEW in October 2015, they were only asked of the full survey sample from October 2017 and were only granted National Statistics status in March 2018.

Figure 2.3. CSEW computer misuse offences (000s)

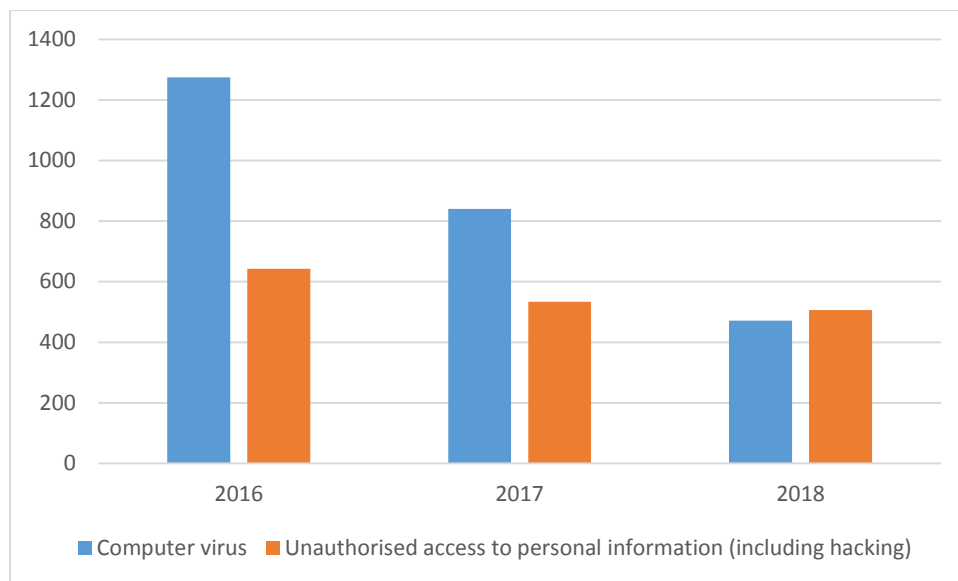


Table 2.1. Computer misuse offences recorded by Action Fraud/National Fraud Intelligence Bureau for years ending December 2015-2018

	2015	2016	2017	2018
Computer viruses/malware ²⁵	4,081	5,208	7,924	5,303
Denial of service attack	246	579	325	259
Denial of service attack (extortion)	134	400	286	224
Hacking - server	506	610	681	845
Hacking - personal	2,331	3,358	3,537	3,996
Hacking - social media and email	5,275	4,484	7,631	9,033
Hacking - PBX/dial through	572	524	364	230
Hacking (extortion) ²⁶	800	1,071	1,005	3,793
Total	13,945	16,234	21,753	23,683

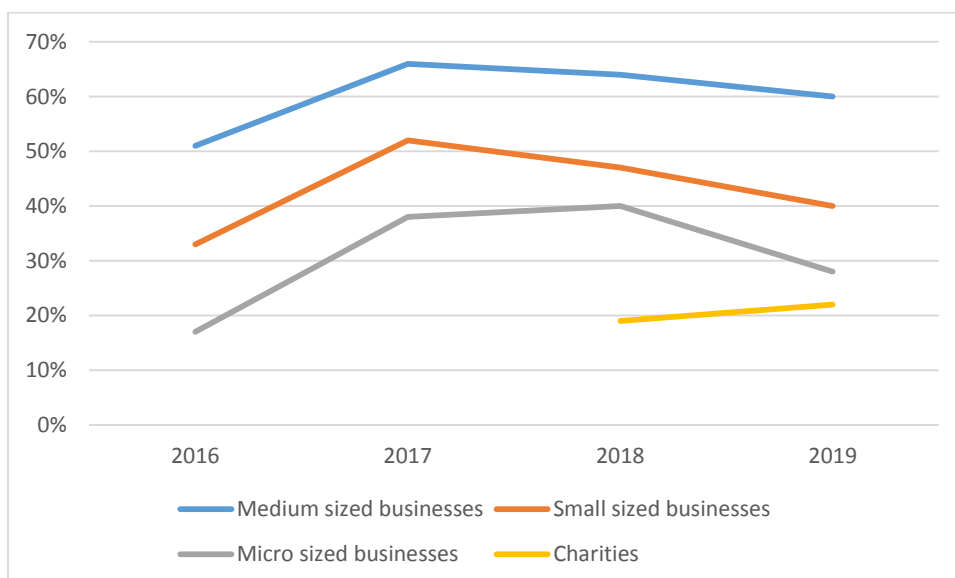
The Government also publish a tool which enables the number of judicial outcomes to be identified by offence (HM Government, 2019). Table 2.2 illustrates the very low number of cases that end in a judicial outcome with in recent years around 50 on average convicted and a similar number cautioned. When compared to the CSEW estimates for 2018, the overall attrition rate (the process of reduction in cases from the total number that occur through to those that result in a criminal justice outcome) is 0.01%. However, it must also be noted computer misuse offences are often used to perpetrate more serious crimes for which the offender is prosecuted.

Table 2.2. Number of judicial outcomes for computer misuse offences 2008-2018

	08	09	10	11	12	13	14	15	16	17	18
Cautions issued	52	63	46	71	66	44	60	74	55	62	51
Proceeded against	17	19	10	11	25	55	53	57	60	64	51
Convicted	12	10	18	11	27	40	38	35	60	47	45
Sentenced	13	10	18	11	27	39	36	39	60	47	46

Another source of data is the Government’s annual Cyber Security Breaches Survey. This seeks a wide range of data relating to cyber security experienced by businesses (and charities from 2018) and the strategies they have in place to deal with it. Figure 2.4 below shows the experience of cyber security breaches of small, medium and micro sized organisations, as well as charities. It shows a significant percentage of micro, small and medium sized businesses have experienced a breach, with around 60% of medium sized and 40% small. However, there is no attempt to estimate how many breaches went unrecognised, or to place ‘value’ on the threat posed by the attack. Therefore, minor breaches are counted equivalent to major ones.

Figure 2.4. Businesses by size experiences of cyber security breaches



Klahr et al (2016 and 2017), Finnerty et al (2018 and 2019)

3. Methods and Profile of Victims

Methods

The research for this report involved the following methods: literature review, stakeholder interviews, survey of victims and interviews with victims. The researchers approached a number of key stakeholder organisations to participate in this research to identify key issues for the research with victims and to assess the landscape of reporting, support and investigation of this type of crime. Interviews were conducted with representatives employed by the following:

- Action Fraud/NFIB;
- NGO focused upon pensioners;
- NGO focused upon victims of domestic abuse, sexual violence and stalkers;
- Victim Support;
- Police constabulary;
- Regional Organised Crime Unit; and
- Large organisation with several thousand employees.

An online survey was devised and 252 responses were purchased from Qualtrics who used their standing panel to find victims of CMC offences and it therefore represents a non-probability convenience sample (Etikan et al, 2016) and therefore should not be regarded as representative of the wider population of fraud victims. A wide range of data was sought and this report will only refer to some of the most important. Respondents were asked to comment upon the CMC incident which had been most serious in the previous two years, which in the sample included:

- 49% - hacking of an online account to access personal information or services [email, social media, bank account etc.];
- 13% hacking of a computer or other device in your possession [laptop, smartphone, desktop computer etc.] to access personal information;
- 29% - a computer virus, or other form of malicious infection, which caused damage or disruption to your device;
- 8% - ransomware - where a form of malicious software caused your device to malfunction and where the perpetrator requested money, or another form of ransom, to restore your device's functions; and
- 1% - denial of service attack - where your internet access was deliberately disrupted, or services and information you provide on the internet were deliberately disrupted [e.g. your website or blog was crashed].

The researchers used a non-probability purposive sampling approach to secure victims to interview. The aim was to secure a diversity of victims based upon the different types of CMC offences, reporting and non-reporting victims, individual and small and medium sized enterprises/organisations (SME/O) victims, an assortment of demographic profiles and from the regions and nations of the United Kingdom. These victims were secured through the following means:

- Lists of victims supplied by the National Fraud Intelligence Bureau;
- Contacts supplied via police force and National Crime Agency;
- The University of Portsmouth Cyber-Awareness Clinic;
- Promotion of research through professional networks;
- Promotion of research through Qualtrics survey;
- Promotion of research on University of Portsmouth website; and

- Some victims were identified in the media and where possible written to asked to participate.

The list of all the victims with their pseudonyms; type of victim; where SME, their activity and the type of CMC offence(s) experienced. In total 52 interviews took place including 38 with individual victims and 14 SME/Os. One SME refused an interview but offered to provide written responses to questions (which they did for several in some depth). That victim has been given the name Mary and included in some tables because of the important information provided. Interviews were largely conducted face-to-face with a small number conducted by telephone/skype where the victims preferred that or they were abroad on business or had emigrated since the incident.

Profile of victims

Appendix 1 provides a full list of the victims illustrating whether individual or SME/O, the type of offence experienced, the devices affected and a brief note on the consequences. It shows

- 7 computer virus/malware victims;
- 7 ransomware victims;
- 34 Hacking victims (or where hacking primary offence);
- 2 denial of service;
- 2 multiple; and
- 1 harassment.²

The literature review highlighted ONS data which showed:

- Higher rates of victimisation among: men, professional and managerial classes, those with degrees and diplomas, unemployed and
- Lower rates among: those aged 75+ , retired.

Appendix 2 compares the key demographics of the survey/interview victims. Both individual and SME victims have been combined, because in most of the SME cases they were micro organisations that the interviewee was largely responsible for and they had dealt with the incident. Both survey and interviews had slightly more females than males. Over 75s accounted for only 1 response in the survey, but 7.7% of those interviewed. The interviewees were also more educated and higher status in occupational status. There was also a bias towards the South East. Table 3.1 provides an overview of the type of offence and what happened in terms of reporting and police action. It shows only 4 with a criminal justice action, 13 with any police interest and with the majority either not reporting or reporting and receiving no police interest.

² Adds up to 53 due to inclusion of 'Mary' who wasn't interviewed, but supplied detailed written response.

Table 3.1. Interviewees by type of CMC, reporting type and response

	Non-Reporters to Any Organisation	Reporters to Non-Police Organisations	Attempted Reporters to Police/Action Fraud	Reporters to Police/Action Fraud – No Further Action	Reporters to Police/Action Fraud where Police took some Action	Reporters with Criminal Justice Outcome
Hacking (bank account)		Charlie, Harold		Henry, Bernard, Hilda, Michael	Claire, Caroline	Sarah, Benjamin, Natalie
Hacking (non-bank account)	Jackie	Andrew, James	Husky, Sam	Peter, Ann, Liz, Alex, Cameron, Angeline, Joana, Jerry, Paul, Kathy , Justin	Catherine, Patricia, Kate, Leo, Mathew , Authur	Sophie
Ransomware	Steve		Aliya	Ralph	Nigel , Sabrina , Arnold , Mark , Kellie	
Computer virus/malware/spyware	Vanessa, Gweneth, Jing, Oliver		Lily	Terry, Godfrey		
Denial of Service		Rachael , Guy				
Other			Wayne			

Black = individual victims, [blue](#) = SME/O victims.

Caveats

Some caveats with the sample should also be noted. First some interviewees could not recall in detail the circumstances of the case. Their recall of some parts was hazy in some cases. There were a number of issues with the designation of what type of offence had actually occurred. Victims do not always understand what type of offence has occurred against them, only that something bad has happened or could have. There is a particular misunderstanding with hacking. For instance, one interview was terminated early because once it began it was clear the victim had not been hacked. An offender had sent emails to his friends/colleagues seeking financial help using an almost identical email to his own. The victim had not been hacked, but his identity had been used as a means to defraud others (although the impact and feelings might be the same). In another case a victim approached the team who had paid an invoice to a firm, whose email account had been hacked and then used to change the details of the bank account for it to be paid. The firm was the CMC victim, not the individual, who was a victim of fraud.

Another important caveat is that at the time of the research there was a pilot of the Economic Crime Victim Care Unit (ECVCU) in London, the West Midlands and Greater Manchester where more intensive support is provided. None of the victims for this research were covered by this scheme.

There was also some issues with the lists of victims supplied by NFIB as the NFIB code listed did not always match what had happened to the victim. The scope of the victimisation of the sample supplied preceded a new system NFIB had recently implemented. Some of these quality issues, may therefore have been addressed, but it was clear that victims responses, particularly in relation to the web had not been quality checked in the past. The researchers, however, also found some issues with those reported by telephone too. Some examples of discrepancies are illustrated below:

- Peter (NFIB52C - Hacking - Social Media and Email). Peter was receiving large amounts of spam mail which he thought was the result of a hack of one of his accounts. This seemed unlikely. Could possibly be classed as denial of service attack, but probably not enough emails to amount to that.
- Hilda (NFIB51B - Denial of Service Attack Extortion). In reality this was probably an attempted fraud that may have involved hacking/malware. There was no recollection of extortion.
- Terry (NFIB50A - Computer viruses/malware/spyware). Terry received a text to a false DVLA website. Under Home Office counting rules if the victim clicks on link and the computer is infected this would be appropriate classification, but although Terry clicked on link no clear evidence of malware.
- Cameron (NFIB52A - Hacking – Server). Cameron had received phishing emails targeting his bank account details. The case similar to Terry, if clicked on link and malware. But no evidence of that and classified as Hacking of Server, not computer virus malware.
- Wayne (NFIB52C - Hacking - Social Media and Email). This was actually harassment via signing Wayne up to unwanted websites to receive emails he did not want, such as the BNP. Without access to a real account of his this, is difficult to classify as hacking as they were just using his email address.
- Some ransomware victims were classed across Hacking (Extortion) NFIB52E and Computer Viruses/Malware/Spyware NFIB50A.

4. Victims' Views on the Recognition and Perceptions of Computer Misuse Crime

CMC offences are relatively new crimes about which there has been only limited research. They are also crimes that often do not involve a direct financial loss or involve direct physical harm to the victim. Such characteristics and the large levels of non-reporting to the police/Action Fraud could lead some to the conclusion they are lesser crimes compared to traditional volume crimes like burglary and vandalism where harms, physical and financial, are clearer. The research sought the views on the status of CMC offences so it is important to start the discussion of the findings with evidence of how serious this crime is considered and then, in the next section, the impact of the crime on victims. These will help to put into context the later parts of this report and the response victims receive.

The survey sought the views of victims on how serious CMC offences were in comparison to other more traditional offences such as burglary, theft and criminal damage. On a scale of 1 to 20, with 1

being a very minor crime like theft of milk bottles from a doorstep to 20 being the most serious crime of murder, asked victims to rate the following offences in table 4.1.

Table 4.1. Survey respondents' views on the seriousness of computer misuse crime

	Male	Female	Overall
	Mean	Mean	Mean
Burglary	9.29	9.64	9.48
Hacking for thrill	7.92	8.54	8.26
Hacking to view PI	8.79	9.14	8.98
Hacking for fraud	10.73	9.95	10.30
Hacking for voyeurism	11.29	10.91	11.08
Sending a virus	9.21	9.56	9.40
Sending ransomware	11.38	10.8	11.06

The table shows the most seriously rated was 'hacking for voyeurism', closely followed by ransomware. These and hacking for fraud were all rated higher than burglary. A computer virus was rated about the same as burglary, with hacking for thrill and to view personal information only marginally lower.

Victims had a great deal to say on this issue and the majority regarded computer misuse crimes as equivalent if not more serious than burglary. There were some, however, who rated it lower. Some of the views of victims are presented below.

Figure 4.1. Interview victims' perspectives on the seriousness of CMC

A Lesser Crime
<p>But I find things like that quite minor, like they're just irritating, they're not doing anything serious. But, if it's obviously more severe, in terms of, like, somebody could potentially steal your data, somebody could hack into your bank, then obviously, I'd cast that as more serious. Vanessa. [Computer Virus, Individual].</p> <p>I don't think computer misuse is as bad because obviously burglary, people have been into your house and they've rooted through your things. Okay, someone's been into my computer and they've rooted around, but they haven't physically touched things or... Liz. [Hacking, Individual].</p> <p>But again, I just feel like, you know, someone going into the physical space of the computer, is not going to stop me from using the computer, whereas someone coming into my house, burgling my house, is likely to make me want to stop going into the house. Does that make sense? Paul. [Hacking and Denial of Service Attack].</p>

I think it's less important than burglary. I mean, burglary to me is a potential lead into violent crime. You know, if somebody had to be burglarizing the place here and I had to come in for whatever reason and catch the person in the act, you've then got quite a high potential of some sort of violence happening. I think theft, fraud and what was the other one? Arnold. [Ransomware, SME].

An Equivalent Crime

[burglary] It's virtually the same thing. I think it's the same thing, because you're stealing someone's property. It doesn't matter if it's an object you can see or an object you can't see, it's still stealing. Ralph. [Ransomware, SME].

I think they're as serious. Sabrina. [Hacking, SME].

Well, it's the new burglary, isn't it. Not through living here, although I have been burgled here but you don't expect to be burgled anymore, you expect this sort of stuff to happen. Bernard. [Hacking, Individual].

To me, it felt the same as if they had been in the house, you know, it was personal, so I felt that they had. And the fact that they'd been on to my... You know, they could get access to my phone and everything, I felt like they had been in the house. So to me it's... Claire. [Hacking, Individual].

I think it's as important, equally important to criminal damage. I would so equally important to theft, equally important to fraud and what was the last one? Arnold. [Ransomware, SME].

So, I don't know, they are very different crimes, but at the same way, in one way they do affect you, there is no question about it. It's a violation of you and your belongings and the way you do things, and I think that can be very hard. Sarah. [Hacking, individual].

A More Serious Crime

Oh, way above burglary. Because burglary is a physical action that, to an extent – I mean, if somebody wants to get in they'll get in – but to an extent you are a master of your own destiny with that. With viruses and the like, it's technology and that's brain power and way beyond the likes of a simple person like me. So, you know, I rate viruses and what-have-you way above burglary, way above. Henry. [Hacking, Individual].

I feel they are more serious because the person who commits the crime feels like there is no recourse for their actions. They feel like once they've done it they feel like they're completely untraceable, they're completely untouchable. Alex. [Hacking, Individual].

I would say it's a lot more serious. But then, I would say that, because the biggest event here has been the computer fraud. If we'd had a really awful burglary where everything was smashed up and everything was trashed, then my answer would probably be different. The burglaries that we've had, I've learned from every single one of them. But they're largely an inconvenience. They

cost more money in terms of replacement of windows, but it still doesn't add up to the 9,000 that we lost... Natalie. [Hacking, SME].

Oh, far higher than burglary. 'Cause, I...burglary, these days, what can you steal from a house, you don't have cash, you've got a television, who wants a great big television you can get them really cheap now. What can you steal from a house, jewellery, I don't have any jewellery so no, I think, hacking you can take a lot more. Joana. [Hacking, individual].

Oh, it affects you emotionally so much and also you're completely unaware that it's happened. So, yeah, I do think it's right up there with the most invasive things that can happen to you personally as well, particularly when you are SME, and I know I keep going back to that but generally in SMEs the owner of the business or the person who's most culpable is generally really heavily involved as well. So you do take it home whereas for bigger enterprises it's not as... But, yeah, no, I would rank it right up there with...it has a huge impact. Mathew. [Hacking, SME].

I think it's probably more serious, because it's hard to detect at times, so it can be operating, and you're not even aware of it. Kellie. [Ransomware, SME].

I believe it affects the person more long term. Criminal damage, you've got insurance, you can replace the things quicker, where cybercrime it takes longer to recover, I find. It's still affecting me this far on, it's almost a lifetime thing you've got to deal with. Where criminal damage, you can call up your insurance company, get it repaired, done. Cybercrime is more complicated than that. Sam. [Hacking, individual].

Yeah, oh definitely, yeah [more serious]. Violating your intimate world, yeah. Kate. [Hacking, individual].

5. Impact of Computer Misuse Crime

The previous section revealed there were generally three perspectives on CMC offences. The largest group noting it is equivalent to traditional volume crimes, with smaller numbers noting a lesser type of crime or a more serious crime. This section will now explore the impact of CMC offences on the victims. It will show many of the impacts associated with traditional volume crimes also apply to CMC offences. The general literature on crime victimisation notes a number of common impacts upon victims and these include:

- Psychological: a loss of self-control, anxiety etc;
- Emotional: fear and anger etc;
- Behavioural: changes to routines etc;
- Physical: bruises, injuries etc; and
- Financial: financial loss (Spalek, 2006).

The experimental statistics brought some quantitative data on the type of impact experienced by victims of computer misuse. It shows the most significant impact was loss of time/inconvenience for both computer viruses and hacking. The next most significant was stopping access to websites, followed by feelings of shame, embarrassment and self-blame. This research identified a wide range

of impacts, which will now be explored. It is also important to note some CMC offences are pre-cursors to other offences such as fraud and there are therefore many similarities in impact to this crime (see, Button et al, 2014).

The survey found that In terms of financial impact where those reported a loss it ranged from £2 to £10,000 with 38.9% of respondents reporting a financial loss with a mean among them of £657 and a median of £250. The far more significant impacts, however, were the non-financial impacts.

Table 5.1. Psychological impact upon survey victims

	A great impact	Any impact (great deal or fair amount)	No impact
I experienced stress	34.5%	75.0%	24.2%
I experienced anxiety	25.4%	70.2%	29.0%
I experienced fear	21.0%	52.0%	47.6%
I experienced anger/violent thoughts	13.9%	48.0%	50.8%
I felt isolated	14.3%	42.5%	56.0%
I felt embarrassed/ashamed /self-blame or similar	17.5%	50.8%	48.8%

Table 5.1 shows the majority of victims experienced emotional impacts. Stress and anxiety were felt by over 70% of respondents. Around half experienced thoughts of anger or fear. Table 5.2 also shows around half experienced sleeping problems or fatigue as a result of the incident. Two fifths experienced depression and a fifth to a quarter self-harm or suicidal thoughts.

Table 5.2. Health impacts on survey victims

	A great impact	Any impact (great deal or fair amount)	No impact
Difficulty sleeping/fatigue	22.6%	53.2%	46.0%
Change in appetite/weight loss/weight gain	8.3%	38.1%	60.7%
Stress-related illness/condition	13.5%	41.7%	56.3%
Panic or anxiety related illness	14.7%	45.2%	52.8%
Depression	16.3%	42.9%	55.6%
Self-harm	8.3%	23.4%	74.6%
Suicidal thoughts	8.3%	20.2%	77.8%

The interviews confirmed a similar range of impacts upon victims and provided more depth to the negative experiences of victims, as well as highlighting the severe impact in some cases. These impacts will now be examined with quotes from interviewees to further illustrate it. Before these are examined, however, the quote from Husky below illustrates what many victims felt.

And it's not always or only about money, there are more important things than money. Yes, there is more important things than money, but there's all different feelings that go into it, from the isolation, from the betrayal, from hopelessness. Husky [Hacking, Individual].

Financial

Many of the individual fraud victims did not experience any financial loss directly or indirectly. Indeed, for some of the victims, financial gain was not the purpose of the crime perpetrated against them. Husky claimed a substantial loss as a result of her estranged husband hacking her laptop, but it is difficult to determine to what extent this is a consequences of the hack:

I said, okay, I've got to think about it. In terms of the outcome of my divorce, I think that I probably lost in the region, of probably £50,000, yeah. Plus all the cost of going to see a solicitor about something, it was like £350 an hour, so at the end, probably I would say, between £50,000 and £60,000, yeah. Husky [Hacking, Individual].

Alex experienced a very small loss as a result of the hacker testing whether he could make purchases:

He bought a very low priced item [59p] on my account to check that he could buy things on there. Alex [Hacking, Individual].

Many individual victims did experience a loss, but were then reimbursed, but at the start of the incident it was not always certain they would be and initial losses sometimes caused financial pain.

Sarah's bank accounts were cleared out and she had no money left, which was problematic as she was due to go to Scotland the next day:

...I was going to be away from home in a hotel for the rest of the week with relatives in Scotland, I literally had about £5 in my purse because I had been intending to go to the bank on the way. And, knowing that I couldn't take any money out of the bank because there was nothing left was a bit shattering. Sarah [Hacking, Individual]

Claire was hacked and lost £7000 initially, taking her down to her maximum overdraft. She was subsequently reimbursed by the bank, but her partner had to help her in the short-term:

Yeah. Well, I had to get £600 off [my partner] to put in my bank account because it happened just before my next... They emptied it right down to my overdraft of £1,700, so they left me with nothing, and then our mortgage was due to go out and other payments and nothing would have... And I was scared of all the bank charges and that, so I had to borrow some cash. Luckily, she had some savings, so I had to borrow off her to just tide me over. And because all my accounts had been frozen, she was just giving me cash so I could get to work and get fuel and just things that you take for granted every day when I couldn't get access to anything. Claire [Hacking, Individual].

For most of the victims where there was a financial loss it was the costs of dealing with the incident and enhancing security afterwards:

Yes, I had to buy Kaspersky of course and pay for my computer guy to go and de-bug it. And so I suppose the financial implications were somewhere around £300. Henry [Hacking, Individual].

I had to take it to PC World to be cleaned and whatever they do. I had to pay for that obviously. I think I paid about £50 in total because my virus thing was out of date, so they updated everything while they were on and cleaned it all. Claire [Hacking, Individual].

I'd say it's almost coming up to a £1,000 for the extras... Sam. [Hacking, individual].

Disruption

The disruption and time that it took to deal with was a major impact for many victims as the experimental statistics of ONS also found. The responses below only relate to individual victims and this issue will be explored later in this section separately for SME/Os:

Very disruptive, so it was literally like, everything you logged on, into a search engine, it would direct you to these sites and then it would keep just, basically, popping up with these adverts every ten seconds, basically. When you're trying to do academic work, you can imagine it's quite disruptive and irritating. Vanessa. [Computer virus, Individual].

No, it was just the inconvenience that, like I said to you, I think I cancelled... Literally, I didn't do them all at once. I rang the credit card companies up because I got a couple of cards. We pay them off every month, but there's nothing... I rang them up to just, sort of, say look, I've been hacked, you know, maybe put a note on my account and then can you order me a new

card and that's the reason. So, like I say, I've had a new everything just to be on the safe side. I'd say it was probably about a couple of hours, you know, ringing up, going through security, this, that and the other, explaining it. Caroline [Hacking, Individual].

God. On the Saturday and Sunday, that was probably about six, seven hours, just for the eBay and PayPal. Facebook was just...that was at least six hours on the day, speaking to Action Fraud and the police. And going on and off and trying to do stuff. And then ongoing messages to them. So easily...I'd say 32 hours, I'd say. Catherine [Hacking, Individual].

It's massive, the disruption in fact is massive. Rachael. [Denial of Service Attack, Individual].

Anger

Anger was mentioned by several victims. This was often directed to the offenders, but sometimes the relevant bodies, institutions and even to themselves for falling victim to the crime in the first place:

Yeah I think for a couple of days I just couldn't stop crying and I felt so low, but after that, I think it did turn more to anger and wanting to fight to get my money back, and also to stop it happening to other people. Claire. [Hacking, Individual].

I just really wish that it had impacted him more so than it has because of what he tried to take away from me and my family. Yeah, I really...I wanted him to suffer, and maybe that sounds petty, but he put me through hell for a few months, and he invaded my personal world, and tried to take away my future and my kids' future, that's the way I saw it. Sophie. [Hacking, Individual].

The other impact of course is a feeling of anger, I suppose, that someone would put you through such inconvenience in an attempt to extort money from you; so mostly it was financial. I didn't need any counselling. I mean it was just bloody annoying because when you've got work to do you want to get on, and some little oik has caused you to lose half a day's work. Steve [Ransomware, SME].

Anxiety

Some mentioned anxiety about the potential consequences of the attack, whether they might be victims again and if the offenders might even visit them:

Probably for the rest of the day. It happened, like, midday and then for the rest of the day I just felt a bit insecure. I don't think I barely went on my phone for the rest of the day. James. [Hacking, Individual].

I was hyper-sensitive to anything that I didn't recognise. And whereas you get these stupid emails, as we said right at the outset, anything that ordinarily I would not think about, I became hyper aware of. So emotionally I was very, very sensitive to any possibly abuses or possible invasions into my privacy. Henry [Hacking, Individual].

Not that I'm aware of but it does make you almost apprehensive to open student emails now which is a bit...it's not a good situation to be in if your students are then emailing you and maybe you're not opening their emails. Gweneth. [Individual, Computer virus].

...I was really really worried, I was thinking, Christ what else are they into are into my PayPal, you know, how many years is this going to be, I mean, does it mean that they're going to be, you know. And, I still don't quite know, you know, whether...how much access they might have to my information, you know? Joana. [Hacking, individual].

This was also an issue for some SME/Os:

I was frightened. I was frightened it was going to happen again. Yes. I was frightened that whoever had done that would know we were vulnerable and probably easy access and might find another way in. Kathy. [Hacking, SME].

Stress

Stress was also mentioned by many victims:

Oh, very stressful. I couldn't work. I didn't have time off work, I just sat at my desk and stressed, not getting work done. Alex. [Hacking, Individual].

It was quite stressful. And I was quite glad that it actually happened on a day that I didn't actually have them here. They were both at the pre-school and school. So it was easier to deal with 'cause I just spent the whole day on the phone and trying to deal with it. Catherine. [Hacking, Individual].

Yeah, it was terribly stressful and it made me feel attacked. Rachael. [Denial of Service Attack, Individual].

Stress was a particular issue for some SME/Os where financial implications or the performance of services were imperative:

It is stressful, it is frightening in lots of ways. And it's very distressing that something you could work on for two years, can just, in a heartbeat, disappear. And we had not realised that. It had never occurred to me that something you put on the internet, doesn't automatically stay there forever. It could just be destroyed and taken away, or removed, unless you keep a copy of that, like any other form of information. Sabrina. [Hacking, SME].

Yeah, I mean, that...so, I was probably up till midnight on the night it happened and that, that was probably the most the most stressful four hours of my career. And I came in, in the morning fully expecting to get sacked because at the end of the day it's my webserver, it's my responsibility to ensure that this, you know, doesn't happen. Justin [Hacking, SMO].

Yeah, it's incredibly stressful because, like I was saying earlier, on about the milestones that the payment card industry set throughout the investigation process that you have to achieve and, unfortunately for me, I was going on holiday right in the middle of it. Mathew. [Hacking, individual].

Embarrassment and shame

Embarrassment and shame was another consequence frequently mentioned, particularly by those whose victimisation related to social engineering:

Just embarrassment really. Ringing up the bank and saying oh yeah, I've been a victim of... It's just embarrassing to admit that you've been subject to something which is so simple. Charlie. [Hacking, Individual].

I was embarrassed because the IT team said, why did you click on it, you should know better. Which I should have known better. Gweneth. [Hacking, Individual].

Well, I wouldn't say embarrassed. Well, in front of some friends rather embarrassed because know-all friends were like, you should've put the phone down. Yes, I suppose I did. Bernard. [Hacking, Individual].

I was embarrassed because various people in work, because of my job, I have... It's a funny area, being a vicar, because your sort of personal life and your working life mingle in a way that they probably won't do in other professions. So on my personal Facebook, there are people, with family, like my cousin, but there are also lots of parishioners as well, who'd got this message and really thought for a minute I was asking them to do something that was, you know, that wasn't quite right over a Facebook message. So that was why I was embarrassed, to have to then tell these people, no, it wasn't me, it was somebody who had taken over my Facebook. Plus, at the time, I was working on the Facebook page for our church and I was telling them how to be...how careful we had to be and security, and somebody had actually somehow had got my Facebook details and logged in and sent this out. So, yes, it was just the embarrassment of the situation. Angeline. [Hacking, Individual].

Yes, I think – yes, course, I was embarrassed about BNP and stuff... Wayne. [Harassment, individual].

Isolation

Some victims mentioned feelings of isolation as an impact of the crime, this was particularly related to the feeling that nobody was doing anything about the incident or seeking to help them.

It's like hello, somebody's just broken into our house and stolen all our things and nobody wants to know. Kathy. [Hacking, SME].

I then felt, afterwards, there was just nothing that could be done about it and it wasn't taken particularly seriously. In the grand scheme of things, you know, how serious was it? You know. Looking at it like that. But I would say I felt isolated. Angeline. [Hacking, individual].

Husky felt particularly isolated as the police would not even accept her case in the first place:

Yes, there is more important things than money, but there's all different feelings that go into it, from the isolation, from the betrayal, from hopelessness. Husky [Hacking, Individual].

Damage to reputation

Hacking and the leaking of personal information can damage the reputation of the victim. If there is sensitive personal information and this is leaked into the public domain, such as marital affairs, sexual preferences, pornography, political views etc which are held in accounts, files etc this can be damaging to the victim. Alex was worried about the damage the perpetrator was doing to his reputation:

I definitely wasn't fearful...like I wasn't afraid that he was going to show up in real life. But I was afraid that he would find the means to escalate this, to either present misinformation about me to get me listed, to get me targeted, something like that. One of my fears is that he would use the limited information he had about me to misrepresent me online, and I thought that the fact that he was pestering me for more than 12 months meant that he was a serial abuser. Alex. [Hacking, Individual].

Patricia was very worried about the damage to her reputation and the impact of that:

And you would genuinely think...and the online stuff, I mean, it's very difficult to get work. I've just finished a book [inaudible 0:43:04] which is the [name of book], and I have said to them, you're going to have to take my name off the front of there and [inaudible 0:43:18] because I cannot, you know, spend the rest of my days thinking that these arseholes are literally going to carry on doing what they're doing, you know. Patricia. [Multiple, individual].

Leo, as a Councillor, was also worried:

Yes, it did affect my reputation because I was a councillor ... in the [location] area, and I was going to stand for election this year but because of what's gone on if I stood for election this would be made public. Leo. [Hacking, individual].

Sophie was worried the incident would damage her reputation with her new employer.

And of course, also with that, the fact that I knew my new employer, it made me feel even worse, because you know, he'd probably chosen me over and above other people, because of our previous history, and then for him to be, in effect, let down so badly, before I've even started, that's horrendous. Sophie. [Hacking, Individual].

Negative changes in behaviour

Changes in behaviour will be considered in more depth later in the report. However, as an illustration here the impact for some did lead to negative changes in behaviour as the case of Sam illustrates below:

It obviously made me feel very vulnerable. I don't do things like Skype anymore, I don't have any of that, so my webcams are now covered. We have a CCTV camera in our house but if we're in where it's placed, it has to be turned off when I'm in the room. I can't have any cameras actually focused on me because it just makes me paranoid who's watching. Sam. [Hacking, individual].

Violation of digital self

An important finding is that several victims viewed the victimisation as a violation of their digital self. The growing use of IT devices and their importance in our lives for many means they can be considered a prosthesis to our physical being. For some, attacks on these devices were considered equivalent to physical attacks.

Some of the victims that noted the most serious impacts identified feelings of violation. For some of these victims the impact was so serious they compared it to rape. Henry compared the incident to having been 'raped' and the violation of his intimate private working space was intense:

...I felt as though... I'd been burgled years ago, when we moved into a new house, and the sense of invasion is vile. I can imagine it must be like rape. And so the emotions started to kick in as I realised that they'd come in. And my computer, because I've got a big, powerful PC up there with four screens, because of the writing, and it's very much a part of me. And I get an immense amount of pleasure and satisfaction out of writing, so the computer is very much a piece of satisfaction for me. And to have it invaded like that made me feel really quite ill.

Henry articulated very well the feelings of violation that resulted from the incident:

No question. And, as I say, in part I think it's because of the intimate relationship I have with my computer because of the writing. You know, I don't like swearing but when I'm writing my language is foul, which is the frustration of getting it from there onto the screen. And that's part of the intimate relationship. Whilst the computer was away, I had a notepad and pencil because, you know, the stuff keeps coming into you to write. And I was handwriting it, longhand, and then crossing it out and then rewriting it again and doing something, three or four full pages of writing, for this one idea. And I started to realise just the relationship I had with my computer and how intimate it is, in the ability to be able to do that. So yes, the violation was intense. Henry. [Hacking, Individual].

Kathy just simply compared the secret watching of her to being raped:

I felt raped, you know, that somebody was watching me, so I was like I'm not using that laptop. Kathy. [Hacking, SME].

Husky also felt violated:

I felt powerless, angry, violated in a way, very angry and angry because nobody would listen to it, 'cause I kind of put my trust in the police, thinking that I'd just been kind of dismissed in a way, just another domestic situation, part of a domestic situation... But it's just...it's just much more than somebody, just the action of going into your computer, yes, that you feel violated, you feel that, you know, but it is the damage that it causes in somebody's life. Husky. [Hacking, Individual].

As did Nigel:

Yeah. But you just feel hmm, what's happened here. And then you're sort of violated. Nigel. [Ransomware, SME].

Patricia compared it to a physical assault:

And I think the police are overwhelmed, but I also think they really underestimate the impact on a human being, you know. When it reaches the point where you, as I said earlier, you feel like you've been physically assaulted, then it should be treated as assault of some sort. Patricia [Multiple, individual].

As did Leo:

I felt violated and really upset because I'd lost...I'd literally spent four weeks gathering all the evidence together and I thought it was secure, and did not understand or realise how vulnerable I was storing stuff online. It's like – I'm trying to think of the best way – I feel violated, like someone's done something to my body against my will. I access my online account it feels like they've done that my brain; they've done something to it without my permission. It's like – I'm trying to think of the best way – I feel violated, like someone's..

Kate felt the incident was an invasion of her privacy and made her feel sick:

And so, it felt like my privacy had been exposed, and I didn't know how or why anyone would want to do that. So, the picture was of my boyfriend, who's still my partner, in the bath, but it wasn't a sexual pose or anything like that, he was just blowing a kiss to me from the bath, but with bubbles, but it still would be an inappropriate picture, I'm a professional, as well, and it made me feel really scared to think that somebody could access my private account, and my emails and my pictures, and see that. Kate. [Hacking, individual].

Leo felt they had accessed his body and brain:

[they have] done something to my body against my will. I access my online account it feels like they've done that [to] my brain; they've done something to it without my permission. Leo. [Hacking, individual].

Loss of digital possessions

The digital self can extend to the many personal things that are kept online, particularly things like photographs or things linked to our digital persona such as email addresses, webpages etc. Several victims lamented the loss of these as a result of the incident:

This is like, I've lost all my photos, all my photos from the laptop have gone. But all my videos, with all the NCT work. Every file I've uploaded has disappeared. So we had our sale on Saturday that I haven't actually been able to do, and I'm the co-ordinator. So it was a rubbish... Catherine. [Hacking, Individual].

The other thing I was really annoyed about was I had to change my email address. Now, I'd had the same email, you know when kids have stupid email addresses, it was a normal email address, it was just my name, and I'd had this email address for like 12 years or something. And I had to change it, and I had to close it. And that was annoying, because I liked my old email address. But, at the time, I didn't really know how to deal with the email bomb stuff. 'Cause like I say, I was getting emails just one after the other, just constantly. I probably should have contact Microsoft, but I just thought, close the email, just get rid of it. Paul. [Hacking and Denial of Service Attack].

Health Impacts

A small number of victims reported health issues as a consequence of the incident, often related to mental health, however, some noted physical impacts. Claire had headaches:

I think a lot of headaches and I took a lot of painkillers in those first few days. Yeah, I was hitting the painkillers, if I remember, and all the phone calls, everything going on, I was just all...like your head is just... Claire. [Hacking, Individual].

Some victims had existing conditions which were exacerbated:

To be honest, I suffer with my health anyway, I suffer with fibromyalgia, so it probably just made the pain a bit worse at certain periods of time, not knowing the outcome of things or the initial investigation. Sophie. [Hacking, Individual].

I've got Crohn's disease so that does get flared up with stress. Catherine. [Hacking, Individual].

Well, I have multiple sclerosis, so one of the first things they say to you, is stress is not your friend. Because multiple sclerosis lives in your immune system, so stress hits your immune system and it weakens it. So yes, I was suffering from attacks of fatigue more, generally, my health was less well, my time was utterly dominated by sorting these things out. Sabrina. [Hacking, SME].

Several victims reported mental health problems as a result of the incident:

I just really hit a low. I think it was the morning after and I just said to Claire...I feel so stupid and all this and I want to just curl up and die. And she went, don't you dare say things like that and it's only money, and, you know, all that then. But I did hit a bit of a rock bottom, yeah. Claire. [Hacking, Individual].

Well, at that time I was over everything, at least one on top, I was an adrenalin junkie. So it means that I was having a full time job, two children, court appearances, on average that went on up until probably last year, on two, or three hours sleep a night. Husky. [Hacking, Individual].

Oh, I was awful, if was awful, I felt...I think it's really difficult with PTSD anyway to be, you know, having nightmares and flashbacks and night terrors and anxiety and it was suicidal thoughts and stuff. But then to have this level of persecution, you know, and... Wayne. [Harassment, individual].

Yeah. The doctor said I couldn't cope with what was going on because my mind was racing, I didn't trust anybody, I was going very withdrawn and literally within three months he doubled the dose and that's stabilised me. Leo. [Hacking, individual].

I was put on antidepressants. Sam. [Hacking, individual].

Suicidal thoughts/actions

The survey found around a fifth may have had suicidal thoughts as a result of victimisation. There were a very small number of interview victims that reported suicidal thoughts or actions:

Yeah, yeah, and to me, at times it was – it's going to sound really melodramatic, but at times it was life-threatening to me, this was...anything could happen, I could get an email or whatever and that was me, boom, and I would be a couple of times sat on the bridge wanting to throw myself off a bridge. And I think that was the difficulty with the situation, that when somebody says, you know, because there's no money involved, that just makes it even worse then, you think, hold on, but this is my life that's involved, not money, why is that more important, why is that... Wayne. [Harassment, individual].

Yeah, well, again because I have it as part of my condition, but there were...I remember the day I think that I was registered with the BNP and the EDL, because both of those are organisations that I despise, that really got to me, yeah, and I tried to kill myself three times that day. Wayne. [Harassment, individual].

You know, they pretty much put me...they very nearly put me in a grave, to be honest. And I've been through, you know, a pretty shit time and worked very hard to be well after what happened in [name of country], really hard. Patricia. [Multiple, individual].

SME/O

The interviewees who worked for or ran SME/Os reported many of the same impacts as the individual victims and some of those were noted above. As some were effectively owners of small businesses this is not surprising. However, this section will focus in-particular on the financial, disruptive and reputational impact on SME/Os.

Financial

Most of the victims did not lose any money directly as a result of the attack, but some did lose money having to deal with the incident. Mary estimated the multiple attacks cost her organisation £82,000 in additional costs dealing with the incident.

I would say possibly...about a half day of work time, the following Monday, to rebuild and reinstall from back up, so cost wise, four/five hundred pounds. Steve [Ransomware, SME].

Probably because it's the staff members trying to recoup and with our offsite back up we've got to pay for it. So then there's all the data transfer as well, which this theatre hasn't got the money for, you know, it's like an added cost we didn't need. Probably a good couple of grand. Ralph [Ransomware, SME]. .

all of the software. I paid for all of the software. We access grant funding, so again, there's your other thing, we wouldn't have any, and I prefer for our donations to the site to go to people doing work for us rather than infrastructure, so yeah, it cost me money personally. None of this software is particularly cheap, particularly when you have no budget whatsoever [for computer security]. Sabrina [Hacking, SME].

Then we did, only just recently, we've had to do it. But I did buy Kaspersky [£35] in order to, you know, improve the security. Kathy [Hacking, SME].

Probably around £2,000 or so. We did some rough estimates at the time and tried to decide whether it was worth claiming on insurance and we just, kind of, said look, it was a bit disruptive but it's not such a disaster, not such a massive expense that it's worth going down that route. Arnold. [Ransomware, SME].

Forty grand. Without a shadow of a doubt. The amount of customers that cancelled, bearing in mind, they're paying £200 a month. Then it's your reputation on top which you can't really put a price on that....With a lot of begging, pleading, and everything else, probably about ten days, but cost us thousands upon thousands of pounds. We lost 70 per cent of our customers. Authur. [Hacking, SME].

Disruption

Disruption for any organisation is negative and can have major consequences. Ralph noted the significant disruption the incident caused to the arts venue:

It virtually corrupted all of our files. It did bring the theatre down to its knees, or very close to it, but then we have got like also backup, but because all the computers, they're not the best computers in the world so the antivirus and that lot are not up to date, but it did give us a lot of struggle with that. Because especially being a small theatre and we haven't got the funds for the information technology[inaudible 0:03:10] in. Ralph [Ransomware, SME].

Sabrina also lamented the disruption:

It cost me a lot in time, which wasn't just about time I could have been working on other stuff for the website. Sabrina [Hacking, SME].

Steve lost half a day dealing with the incident:

So, what I did...luckily it was only one machine. It didn't spread across the network. So I shut the machine down. I wiped the hard drive, rebuilt it with a fresh version of Windows 10, and then I had a back up and I restored all the data from a back-up because the best...as you know, the best prevention against these types of attacks is to have your data backed up either offline or in a network location where the virus isn't going to get to. Steve [Ransomware, Individual].

Nigel noted how the disruption could arise weeks or months after the incident:

And it's not until we went out and bought another computer and you're looking at, down here we've got lots of animals, and you're looking for it, I haven't got that document anymore. It's all those little things, it could be months later when you're like, I've got to rewrite that, I ain't got the document for the [animals]. We had a database on all our [animals], when they were born, what [animals] they've had – gone. And they were my only copies. Yeah, lost a lot. Nigel. [Ransomware, SME].

Guy illustrated how the DDoS attacked caused major disruption to the school where staff couldn't do their work, couldn't order resources for the school, they couldn't pay staff or contractors correctly to name some:

So the way that obviously a school works in the modern days, the majority of our resources are stored in the cloud, which meant from the perspective of the ability of teachers first and foremost to be able to access free planned work and all that kind of stuff, it was particularly

difficult. They were having to do stuff from home and print things from home. So certainly workload wise for teachers it caused major issues. From the administration side of the school which is sort of more my area of focus, probably somewhere between I'd say 80 per cent and 90 per cent of the systems that we use in order to process the administration of the school are internet based. So not having the ability to run a financial system for two weeks meant that we couldn't place orders for necessary resources. It meant that we couldn't meet statutory obligations for the government and the taxman and all those sorts of things, from our HR system. It meant that we were unable to access the system to process changes to payroll, so people's pay was affected. There are many, many examples, but those are the kind of things that occurred. During that time obviously our IT guys on site were impacted hugely because they couldn't get on with their day to day work because they spent essentially two weeks working with the council in order to try and resolve the issues. It was two days of complete loss and then up to two weeks if my memory serves me correctly, of intermittent use. So lots of frustrations across the building as you can probably imagine. Guy. [Denial of service attack, SMO]

Reputational damage

Reputation is important to the success of many organisations. Some of the SME/O organisations interviewed reported significant issues here. Kathy's whose business's email had been hacked with the offenders trying to change the bank details customers paid for services reported significant reputational damage:

Well, you know, our name might have been smudged because the doctor [who paid to offender's bank account] might then say, huh, [x Gas and Plumbing], bad experience, wouldn't use them again. Yes, they did the work but it cost me five grand to have a new boiler put in. Because he paid once and it went to the fraudster, then he paid us again, so... Kathy. [Hacking, SME].

She went on:

No, but a lot of our business is by word of mouth, recommendations. And he'll never deal with us again... Kathy. [Hacking, SME].

Some of the SMEs operated in IT and becoming a victim of cybercrime was very embarrassing and potentially damaging:

Perhaps, well, certainly, from a professional point of view yes, you know, when you're in the IT industry and you become the actual target, yeah, is... Mark. [Ransomware, SME].

Mathew, who ran an online retailer, was very worried the hacking of his website might result in lost customers:

But in the back of my mind for the whole time I'm thinking, are we going to lose any customers from this? Going through the list of credit card information they'd sent us through that had been cloned from us some of our best customers' names are on the list. So that was obviously at the back of my mind as well. And then also thinking you do feel like you've been burgled. So, yeah, it's stressful. Mathew. [Hacking, SME].

For Justin the linkage of the school website to a porn website was obviously damaging and caused damage to the school reputation:

[the redirection] had quite a big impact in terms of pupils saw it, word got around to pupils. So, lots of pupils were going on it, parents saw it, lots of them were, you know, for the next few days were contacting the headteacher with understandable concerns that this stuff had been, you know, accessible on a school-owned domain. Justin. [Hacking, SMO].

No significant impact

The focus so far has been upon a variety of impacts. However, it is important to note that there were a small minority of victims where there was no significant impact with very few of the impacts listed above. The incident was nothing more than a minor inconvenience, which caused disruption such as having to reset a password or deal with a computer virus. The sample of victims interviewed is biased towards reporting victims and it is possibly likely that interviewing a larger pool of non-reporting victims might yield more victims with no significant impact with only minor disruption, as noted by the ONS data.

6. Falling Victim

The interviews with victims revealed a wide range circumstances of how they fell victim. Some of the incidents involved the victim having no idea who the perpetrator was or how they had fallen victim. For these victims the random nature of the victimisation left some with anxieties (which was explored earlier). Some of the victims interviewed did understand partly what had happened either clearly or vaguely. There were a number of victims interviewed who had fallen for social engineering techniques of varying sophistication. Some had interacted with the offender(s) over the telephone and allowed them to remotely take over their computer, some had responded to fake emails, some had visited websites that on reflection they thought were false. Some of the victims also acknowledged afterwards they had exhibited behaviours putting them at greater risk, such as having poor passwords or going to websites where there is a high risk of malware. There were also a handful of victims that knew immediately or soon after who the perpetrators were. There were also a very small number of victims who had excellent security knowledge and procedures who were victims as a result of factors beyond their control.

The weak point

Several victims described what could be described as a 'weak point' moment. These victims generally considered themselves to have strong resilience to such attacks normally, but because of unusual personal circumstances on the day of the incident fell for some form of social engineering. Henry was busy writing his book and his mind was focused upon that, so his guard was down when they contacted him and seemed plausible:

I'm just finishing a book and it's at the critical stage now where it's the final editing and you're focusing on every aspect of the book. I repeat myself and so I'm very aware of that and so my mind, on this Saturday mid-morning, was very much into the book and total focus, total concentration. And the phone went and this Indian-sounding chap said, oh it's BT Openreach. We understand you've had some problems with your computer and, because you're a loyal and long-standing customer, we'd like to try and resolve it for you. And I had had some problems with it, not important problems, irritations I suppose more than anything else. And because of where my head was, my whole attitude was, okay, it's BT Openreach, yes, just get

on with it, just do it, fix it. I want to get back to the book. Nothing seemed unreasonable at that moment in time, because I was where my head was. Henry. [Hacking, Individual].

Godfrey was just in a hurry and about to go out, so rushed responding.

And it was also, as I say, there was an element of hurry on me, at that moment. So I probably didn't think as clearly as I should have done. Godfrey. [Computer Virus, Individual].

Victims with poor security habits

Many of the victims, however, did reveal various poor security habits that were likely to make them a greater risk of victimisation.

Passwords

The breaching of passwords by offenders was a common issue in many of the hacking incidents. Some of the victims had weak passwords, some used the same for multiple accounts.

I changed passwords once in a while. Probably not as much as I should have done. It's the whole thing about don't give your passwords to anyone else. But I was still in the fact that one password for one thing is the same for another. So if they knew the password for one thing they'd know the password for everything. Charlie. [Hacking, Individual].

I had a strong password, but I had the same password for everything. Paul. (Hacking and Denial of Service Attack, Individual].

I tend to use the same one across platforms because I'm 63 years old and I can't remember any of them. Cameron. [Attempted hacking, Individual].

Some victims had simple guessable passwords:

I've probably used about four passwords and haven't really changed them. I've only...I used to have one for business and one for personal. And now I just change them to my kids' names really. But that was a bit...then I just changed it a bit more, but I haven't really changed them and changed them and changed them and changed them. We used to do that at college when I was teaching. Every 30 days we use to have to do it. Catherine. [Hacking, Individual].

Liz kept a list of passwords on her laptop.

But the problem being is that I never remember the passwords that I've put in. So, say, for instance... I'm just trying to think. Oh, I have a gardening account and obviously I've saved the password for that. And then if it came to my laptop was stolen and I needed to go into that account to reset the password, then I do have a list of passwords. Liz. [Hacking, Individual].

Anti-virus

Several victims revealed they did not have any anti-virus software on their computers. Vanessa who had been the victim of malware revealed:

So, like, the first one, the really serious one I had, was because I didn't have anti-virus, so I didn't have my Windows Defender, and I didn't have anything like Avast, like, because it

wasn't, like, familiar to me at this time that these were issues. And then, I used a lot of sites where you can stream TV shows and stuff, that obviously are not good to use for your computer, which I can't use on certain laptops. Vanessa. [Computer Virus, Individual].

Ralph revealed the other business priorities of their organisation had led them not to keep anti-virus up-to-date.

but because all the computers, they're not the best computers in the world so the antivirus and that lot are not up to date, but it did give us a lot of struggle with that. Because especially being a small theatre and we haven't got the funds for the information technology so it was like, oh, we'll put [inaudible 0:03:10] in. Ralph. [Ransomware, SME].

Nigel had taken much interest and had just downloaded free software.

I'd download things that were free on the computer and that was it really [before]. Nigel. [Ransomware, SME].

Jing and Lily were both students who suffered from a computer virus, but provided different attitudes to anti-virus. Jing had had free anti-virus on her new laptop fitted, but had let expire at the end of that period. Lily had used free anti-virus. The incident had prompted Lily to pay for what she thought was better anti-virus, but Jing no change.

Alex was dismissive of the benefits of anti-virus software.

No, I don't. And the reason for that is because from all the cursory research I've done there doesn't seem to be evidence of them doing much more than warning you if you download something from a site, basically pestering you if you're on an unfamiliar site, and it's like well, I know I'm on an unfamiliar site, I know I'm being careful. So some of it was me feeling like I knew when I was at risk and being more careful. So a good example of this is if a site looks dodgy I won't access it from my phone because the website can't do much to my iPhone. It can't really install anything. Whereas there are more vulnerabilities on PC. So I felt safer accessing something shady. Alex. [Hacking, Individual].

Risky behaviours

Some victims revealed they engaged in risky behaviours that made victimisation more likely, such as going to illegal websites. Vanessa had regularly gone to unauthorised sites to watch movies and dramas:

So, it was probably from any of the number of sites that I used to stream, like TV things on. Vanessa. [Computer Virus, Individual].

Lily also admitted this:

Yeah. I used to use those online movie websites and I think that that could have sparked a virus or a few viruses. So I don't use them, [or I try not to, 16:29] anymore. Lily. [Computer Virus, Individual].

Lack of engagement with security standards for SMEs

Of the SME/O victims interviewed [or responded in case of Mary] most did not work to any cyber security standards and even worse, many had not even heard of them. Mary reported both before

and after the incidents they were not working to any standards and simply had an information security strategy.

I didn't know about these Cyber Essentials. No, I don't know about them, you've just told me. I'll have to do some research about that. Ralph. [Ransomware, SME].

Victims with good security habits

It is also important to note that there were some victims who had very good security habits, but who still became victims. Alex worked in IT and had good knowledge of what good security was. After the first hack he had upped his security, including adding two-factor authentication to his account, but he was still hacked again.

Yeah. It was clear that he was trying to get more information about me, but what was more scary was the fact that this was several months after the original incident and he was still kind of like a dog with a bone, and he had a kind of vendetta. This actually persisted into 2018, more than 12 months, when he was able to hack my PlayStation account again, despite having a lot of additional security lock downs put on it. Alex. [Hacking, Individual].

Arnold's company contracted IT security to a good company working to ISO27001, but they still experienced a ransomware attack. Although the good quality security and procedures in place probably helped in responding to the incident so quickly and well. Jerry worked in IT had excellent knowledge of IT security:

But it was clear someone had got into my account. Now this is an account that, like most accounts, the log-in details are your email address and a password. All my passwords for every site I use are different, they're normally around a dozen characters long and alphanumeric and symbol strings. And I use a piece of software to keep track because you can't remember it. And funnily enough, now Google does it for you, which is quite useful. But I use different ones for every website so that if I ever get compromised, it only affects one site, unlike most people who use the same here, there and everywhere. But it meant that the problem was limited. Jerry. [Hacking, individual]

He also used multiple anti-virus software packages, yet he was still a victim. Authur also had excellent knowledge and security and the attack happened because of factors beyond his control:

Yeah. I mean, all the servers had individual security packages on them; it was just a flaw in the operating system that they walked through. So it didn't matter what security packages you had on there because they literally had a back door and a key through the flaw in cPanel software. Which cPanel won't admit, but the fact that after I gave them the infected files, within a matter of hours there was X amount of updates done. Basically, the updates were about a year's worth of security updates. Authur. [Hacking, SME].

Victims' response to victimisation

A common sense perspective would suggest that a person or organisation which is a victim of a CMC offences would seek to change security behaviours and the ways things are done to reduce the likelihood of them occurring again. Thus at the most obvious level a victim of a computer virus with no anti-virus software would acquire such software and someone who has been hacked would develop more complex passwords if they had been simple or compromised. The research has found that although this does happen, in many cases it does not. In fact the lack of engagement in changes

in behaviour and the way security is done in many cases was concerning bordering on worrying. This section will illustrate this through both the survey and interview data, using case studies from the latter. It will begin with the impact on security behaviours.

Change in security behaviours

Both the survey and interviews highlighted limited changes in security behaviours in general as a result of victimisation.

Table 6.1. Survey respondents changes in security behaviours

	Always undertake protective routines	
	Before	After
Use password/passcode/PIN to unlock smartphones or tablets.	35.7%	49.6%
Use a strong and separate password for main email account	51.2%	45.6%
Install the latest software and app updates once you notice that they are available	35.7%	41.3%
Turn on and use two-factor authentication (2FA) for your main email account.	34.5%	31.3%
Back up your most important data	24.2%	35.7%
Never save passwords using a password manager on smartphone or tablet	25.8%	13.5%
Never save passwords for websites when given the option in the web browser.	24.2%	13.1%
Report any phishing emails by hitting the Spam or 'report phishing' button in your email account toolbar	24.6%	34.9%
	Usually (always or often) undertake protective routines	

	Before	After
Use password/passcode/PIN to unlock smartphones or tablets.	60.7%	74.2%
Use a strong and separate password for main email account	73.4%	70.2%
Install the latest software and app updates once you notice that they are available	63.1%	71.0%
Turn on and use two-factor authentication (2FA) for your main email account.	64.7%	59.9%
Back up your most important data	46.4%	66.7%
Never save passwords using a password manager on smartphone or tablet	26.6%	23.8%
Never save passwords for websites when given the option in the web browser.	22.6%	20.2%
Report any phishing emails by hitting the Spam or 'report phishing' button in your email account toolbar	54.8%	57.9%

The survey findings suggested:

- Victimization does not cause a major change in protective routines;
- There is a small increase in use of device passcodes, software updates, data back-ups and reporting; and a decrease in the use of device and website password managers; and
- There is no significant change in approach to protective authentication through strong passwords and 2FA for email accounts.

The interviews revealed many examples of victims who barely or some cases did not enhance their security at all as a result of victimisation. This will be illustrated by some figures to illustrate some of these cases. There is not the space to consider all the victims, so some of the most salient examples will be considered.

Getsafeonline provides advice on preventing this type of incident by using the most up-to-date anti-virus software. One would expect someone who is a victim of such an incident ideally to invest in such software. One might also expect the victim to look at websites offering advice and possibly to change behaviours if risky use of computer devices contributed. The following illustrate the different responses of victims to this type of incident. The first three in figure 6.1 show the contrasting responses of three victims who experienced computer viruses/malware. Jing did not change any behaviours, whereas Lily embarked upon a complete upgrade of her cyber security as did Vanessa.

Figure 6.1. Computer virus/malware victims' changes in behaviour compared

Name	Security Before	Victimisation	Response	Security After
Jing	Poor security behaviours including no anti-virus.	New laptop froze due to suspected virus at expiry of free anti-virus. Disruption to academic studies.	Self-help did not consult any websites or seek formal help.	No change. Still no anti-virus. No awareness of websites offering advice.
Lily	Medium security behaviours. Free anti-virus and same passwords used.	Contacted to say malware on computer which had hacked her webcam. This was false, but response triggered by this revealed viruses and malware on her laptop.	Reported to Action Fraud, but no interest or support. Googled what should do and identified a variety of means to enhance security.	Enhanced security, better anti-virus, use of 2FA and awareness of websites offering advice.
Vanessa	Poor security behaviours including no anti-virus.	Malware on her laptop redirecting her to porn sites.	Housemate with IT knowledge helped clean laptop and offered advice.	Wouldn't use device unless anti-virus. But no knowledge of websites offering advice.

Ransomware, as a form of virus/malware, one would expect similar responses as above for computer viruses. The additional context of staff in SMEs one would also expect measures to promote awareness among them, where they are employed and may engage in behaviours putting the organisation at risk. The response of three SMEs is compared in figure 6.2.

Figure 6.2. Ransomware victims' changes in behaviour compared

Name	Security Before	Victimisation	Response	Security After
Arnold	Excellent security procedures and contracted company providing services working to ISO27001.	Ransomware attack, all files encrypted of firm.	IT staff with relevant knowledge dealt with incident.	Excellent response, continued use of same company and anti-virus/firewall updates checked more regularly. Raised awareness of issue with staff.
Nigel	Poor security, little knowledge and downloaded free anti-virus	Ransomware attack, all files encrypted	Discussed with friend, police visit to take report and visit to PC World.	Backing up of more data, return to paper systems. No knowledge of cyber security standards, websites offering support etc
Ralph	Basic security such as anti-virus, back ups.	Ransomware attack, all files encrypted.	Self-help based upon key member of staff's knowledge on accessing backups to put back on computers.	Manual checking of suspicious emails. No knowledge of websites offering support or any cyber security standards.

In many cases the changes in security behaviour were very basic with changes of password and purchase of anti-virus software common. For many of the victims of hacking (non-banking) victimisation related to simple passwords or using the same password for multiple sites (one of which there had likely been a data breach). Catherine was an example of this and as the diagram shows there was still little change. However, her case was recent and she was receiving support from the police and a password manager was been considered. Angeline also provides another example illustrating little change. Paul provides an example of a better response to such an attack.

Figure 6.3. Individual hacking victims' changes in behaviour compared

Name	Security Before	Victimisation	Response	Security After
Catherine	Only two passwords used for all accounts.	Victim of hacking of eBay and Facebook accounts.	After reporting to Action Fraud police officer provided regular advice and support to enhance behaviours.	More passwords used but still simple. No awareness of websites offering support.
Angeline	Basic security: device locking, anti-virus, some shared common passwords etc No knowledge of websites offering support.	Facebook account hacked.	Reported to Facebook and Action Fraud.	No changes in security behaviour No knowledge or visits to websites offering support More cautious accepting friends on Facebook.
Paul	Poor security procedures, same simple passwords all accounts.	Hacking of eBay and denial of service attack.	Reported to eBay and Action Fraud – no help. Self-help to address security weaknesses.	Closed email account. Varied passwords and two-factor authentication for some accounts. Limited awareness of support/advice.

However, knowledge of let alone pursuit of relevant standards, including Cyber Essential was rare among the victims. Most pursued very limited responses to enhancing their cyber security after the incident. Kathy and Natalie who both ran SMEs instigated some changes, but had no knowledge of relevant standards and still had security gaps.

Figure 6.4. SME victims' changes in behaviour compared

Name	Security Before	Victimisation	Response	Security After
Kathy	Basic security procedures.	Hacking of email account.	Reported to Action Fraud (after contacting Citizen Advice) – no help. Self-help to improve security.	Changed passwords. Purchased more expensive anti-virus (Kaspersky). Now aware of Action Fraud and Cyber Aware, but not any standards.
Natalie	Basic security procedures.	Hacking of bank account.	Self-help after reporting to bank.	Dealing with incidents generally more professionally, reliance on daughter for cyber security. But still unsure of authenticity of websites, what a strong password is and cyber security standards.

Some victims either had excellent security or enhanced their security but were still victims. Alex did enhance his security after the first incident, but even with more complex passwords and two-factor authentication he was still hacked again. Jerry worked in IT and had very sophisticated security, but was still hacked – probably as a result of a hack of the provider's website or a corrupt insider revealing details.

Figure 6.5. Victims' with excellent security

Name	Security Before	Victimisation	Response	Security After
Alex	Very good knowledge of security, but not highest applied for passwords for Playstation as considered low risk	Hacking of Playstation account and Twitter.	Worked in IT and had good knowledge what to do to enhance security.	More complex passwords and two-factor authentication, but still hacked again!
Jerry	Excellent security: complex and different passwords for every account, multiple paid for anti-virus, backing up and good knowledge. Awareness of multiple websites offering support and advice.	Hacking of Ali Express account	Worked in IT and had good knowledge what to do to enhance security.	Same excellent security.

The research also sought information on changes in behaviour beyond security. Both the survey and interviews found that victimisation did not generally lead to any significant change in behaviours.

Table 6.2. Survey respondents' change in general behaviours as a result of victimisation

	Change in protective behaviour		
	Significant increase	Any increase (significant or small)	No change or reduction
Less use of device	13.5%	44.0%	54.8%
Less use of internet	10.7%	33.7%	65.1%
Less use of social networking	13.1%	33.3%	65.1%
Less use of online banking	6.7%	28.6%	69.4%
Less online payments	7.5%	32.1%	66.3%
More interest in computer security	13.1%	36.1%	62.7%
Less trust in others	15.1%	44.0%	54.0%

The table shows:

- The experience of harm is unlikely to lead to a significant increase in protective behaviours;
- A minority of persons are more cautious;
- The majority do not change their behaviour;
- Most people who engage with the online world are resigned to the risks, pragmatically; and accepting the risks in exchange for the expediency of online services.

Figure 6.6 illustrates examples of both positive and negative changes as a result of victimisation. However, as indicated above and will be developed more shortly the opportunity could have provided for even more significant positive changes in behaviour to enhance security.

Figure 6.6. Positive and negative changes as a result of victimisation

Positive Changes	Negative Changes
<p>Yeah, it's made me more aware, or even more aware, of the importance of backups; because the biggest loss...I mean there's a figure you can put on how many hours it took to deal with the situation, but the biggest loss, of course, would be loss of data, especially client data, and so it's reminded me of the importance of keeping offline backups, whereby whatever happens, you always know you've got another copy. Steve. [Ransomware, SME].</p> <p>Everything is now passwords, two-step verifications. I'm kind of more aware of what I've logged into, because sometimes it's easy just to log in to everything and never log out, especially on your phone and stuff, you just click it and it just comes up and you're like, oh, I didn't have to put my password in, so much of that. So I'm a lot more aware of what I've got that I automatically log in to and what I definitely log out of after each use, and the same with the desktop computer as well. Andrew. [Hacking, Individual].</p> <p>I'm definitely more aware of not just flippantly clicking on what would be conceived as a dodgy website or one that's not got the padlock on it or not secure. So yeah, it's definitely changed that. That's probably through both studying cybercrime and being a victim of computer misuse as well. Charlie. [Hacking, Individual].</p> <p>Well, no, I ensure now, like I just recently purchased a new laptop and I made sure straightaway that I put the antivirus software on there. Gweneth. [Computer Virus, Individual].</p> <p>Oh, I've lost trust, yeah, yeah. I think it's changed me, yeah...That people can do that, sort of, or that people can do that to somebody, I don't know, I'm quite wary now, yeah. Claire. [Hacking, Individual].</p>	<p>I'm still the same. Peter. [Hacking, Individual].</p> <p>Yeah, it probably is the same but I really need to... I'm going to go home and just be on there all day now today just trying to work out my security. Ann. [Hacking, Individual].</p> <p>I've turned my computer on once since then. But it's got three viruses on it which I haven't had a chance to get rid of yet. So I haven't... Catherine. [Hacking, Individual].</p> <p>I didn't do online banking for a little while. I took in cash to pay for his after school fees and they said, oh, we don't accept cash. Catherine. [Hacking, Individual].</p> <p>Still zero interest in it [cyber security]. It's not the most exciting subject. Paul. [Hacking and Denial of Service Attack, Individual].</p> <p>I just use it for writing letters or backing up my iPad. Since this has happened I don't trust the computer, I don't trust the antivirus to keep me safe, so I just leave it totally separate from the internet so whatever is stored there is there, if you know what I mean. Leo. [Hacking, individual].</p> <p>Yes. The only thing I use now is Twitter. But Facebook, all of that, it went straightaway. Sam. [Hacking, individual].</p> <p>I have a Facebook account but it is locked down and private. It has been [inaudible 0:51:42] I've got rid of a lot of people, [been a cull 0:51:49]. You know, the [awful 0:51:51] thing is, that I've lived and worked all over the place and I've got great friends, and sometimes that connection is...you know, people do only use Facebook or... So I've been really active around saying, like, if you want to contact me, this is how we're going to do it, we're not going to do it through this channel, we'll do this. All of my things like</p>

Oh, my behaviour has definitely changed as a result. So, I am now much more savvy about authentication. I'm much more likely to report things now. And I'm much more likely to try and deter an attack of that sort happening, by having back-up systems and having an alternative. And that, you know, whether I'd use, like a, sort of, provider that could so easily be attacked. Again, I don't know, maybe I would. Although to be fair to Google, they did stop it. Rachael. [Denial of Service Attack, Individual].

Yeah. I used to use those online movie websites and I think that that could have sparked a virus or a few viruses. So I don't use them, [or I try not to, 16:29] anymore. Lily. [Computer Virus, Individual].

Messenger are disabled so that you can't see when I'm online, because that became a way that they could track and monitor me. The same with WhatsApp, again, everything's disabled so you can't see when I'm online. I'm not geo-locatable. Anything I don't...everything is private. I have an Instagram account which, you know, a dozen people I know, really close friends. You know, I think Twitter's a cesspit, Facebook less so but it's easier for people to get you. I think Messenger is also very hackable by all accounts. So I use something else, I use another system which is not Viber, it's [inaudible 0:53:12] my brain's not working, sorry. Patricia. [Multiple, individual].

The missed opportunity

It was clear from the interviews that initial victimisation does stimulate an interest in cyber security and lead to some changes in what the victims do. Generally this point is very close to the immediate aftermath of the incident. However, at this point many victims do not receive suitable advice and support and do not access appropriate sources of advice, such as certain websites like the National Cyber Security Centre's or Getsafeonline. Thus a victim of hacking who had a poor password should be exposed to advice on high quality passwords, using different passwords for different accounts, possible use of two-factor authentication and the use of password managers to name some at the point of reporting. In the immediate aftermath exposure to such advice might be more likely to yield more positive changes of behaviour.

Unfortunately this moment of opportunity seems to be under-utilised. Many victims do not seem to be getting immediate advice, even if reporting to Action Fraud. Most victims do not seem to be going to the better quality websites to secure information or receiving quality advice. The initial spark of interest could be better exploited to get key messages to victims on enhancing their cyber security. Some victims do not change security behaviours at all, making further victimisation likely. Some only change a few minor areas related to the incident, such as most commonly for hacking victims changing passwords. The lack of knowledge of the Government's Cyber Essentials and other related standards for SMEs was also concerning.

It is also clear there are a plethora of websites offering advice. That victims because of the nature of victimisation are wary of websites. Finding advice and technical support is also a challenge as victims find it difficult to determine reputable providers and websites.

7. Reporting Computer Misuse Crime

The report will now start to consider the response of relevant organisations to victims. This section will start to consider the reporting of CMC offences. It will first explore the reasons for low reporting before then examining their experience of reporting and then the response they received.

Reasons for low reporting

Earlier in this report the very high rates of attrition for computer misuse offences were illustrated. The reasons for individuals not reporting has been explored by the experimental statistics from the CSEW for year ending September 2016 were: they had not heard of Action Fraud at 66 percent (the same number for fraud offences too). Thereafter there are differences to fraud with too trivial at 12 percent (compared to 5 percent for fraud), 10 percent identified they dealt with the matter themselves (compared to 4 percent for fraud) and a variety of other responses in very small numbers (these questions have been recently revised).

This research secured data from both the survey and the interviews. The four most common reasons among non-reporters in the survey were:

- 43.3% not having heard of Action Fraud or not realising they dealt with computer misuse related crime;
- 43.3% dealt with the matter themselves;
- 19.2% by the belief the police wouldn't do anything; and
- 18.3% No loss or small loss/felt too trivial/attempt unsuccessful.

A variety of other reasons were noted and the interviews also echoed these key findings among others. The reasons uncovered from the interviews will now be explored.

Status of computer misuse related crime

The starting point for considering CMC is more ambiguous than traditional volume crimes like burglary. These new crimes are not always considered clearly as crimes and there is more uncertainty over their status, particularly where there is no financial loss and for computer virus related offences. The comments of Gweneth and Jing illustrate this:

Well, as far as I know, I don't believe a criminal offence against myself has taken place, I'm not aware of any...if my details have been cloned or anything like that because the work on my computer here just generally tends to be my academic work. Gweneth [Computer virus, individual].

I didn't know this, that it's some criminal case that I can report. Jing [Computer Virus, individual].

There was no financial loss

Linked to the status is the issue of financial loss and many incidents do not involve loss, leading to less interest in reporting:

No, there was no loss involved, 'cause I was just ahead of the game you might say...I don't know what the police could do in cases like this anyway, between you and me, what are they going to do? I mean the guy was probably from the Far East, not in this country. Harold [Hacking, individual].

Oliver also noted this:

So I mean because I didn't hand over my information, I didn't hand over any of my credit card details, I gave them nothing, I didn't report it because I just thought well there's not really much they're going to be able to do, I don't want to waste their time. Oliver. [Computer virus, individual].

Assumption non-police/Action Fraud initial reporting body would pass on

Lots of the victims who did not report to the police/Action Fraud, did report to the relevant service provider. Many of these felt no further action was required if their situation was resolved. Some also assumed the body they were reporting to would pass on to Action Fraud:

Because they said they'd pass it on. They said they'd keep the incident and if it amounts to anything then they'll pass it on to the police, but I never heard anything after. Charlie [Hacking, individual].

Yeah I mean it's something that we discussed as a leadership team and whether or not there was a mechanism in order for us to do so. So we went back through our academy chain and had a discussion and we've reached the point where they essentially said, if the council have said they're doing it, let the council deal with it. But certainly we had discussions around the table as a leadership team to say, what can we do in terms of raising it and the answer back from the academy saying don't do anything. Guy. [DDoS, SMO].

In Benjamin's case the incident had been successfully resolved by the bank, so he did not feel the need to report to the police or Action Fraud:

But given that we'd been compensated within, I don't know, three or four days, I think, we were happy just to get the money and carry on with our lives. Benjamin [Hacking, individual].

Some victims were able to resolve the situation themselves so felt no need to report and seek any further help:

I think it's because I resolved it myself, I was happy with the outcome, that they'd locked it out, that we updated my details and put in the two-step verification thing, they'd explained some more kind of things about security and stuff and changing my password, and the fact that this person no longer had access. That was the main thing. It was kind of like it was resolved, so that was nice. Andrew [Hacking, individual].

Reputation and experience of Action Fraud

The reputation of Action Fraud and past experience was a reason identified by some victims:

all people say about Action Fraud is that it's an easy way for the police to get rid of a troublesome complainant, so they give you a website. You go to the website. You fill out this online form and they give you a number, and you get a generic reply. And you really don't hear anything more. I mean I appreciate the volume of what they must be dealing with. But you feel that it's a bit of a black hole really. Steve. [Ransomware, SME].

This is what Rachael thought too:

...I have reported a different thing to Action Fraud, which is next to useless. I mean, it's worse than useless, it's a waste of your time, for literally nothing. That was a completely different

incident that I've reported to them, where somebody was checking into a hotel in my name, and I was getting things and they were, like...we rang...we actually rang the hotel and they were, like, they've checked in. And I was, like, well go and get them, these people are fraudsters, but Action Fraud did absolutely nothing about it. But no...the 2017 attack no, I didn't report it to Action Fraud. Rachael. [Denial of Service Attack, Individual].

One victim who experienced an ongoing incident that lasted over a year in the initial phase had not only reported to the local police, but also the police where he thought the offender lived. He had also reported to Action Fraud, who had told him to dial 101 and report to the police. As his hometown police had shown no interest, when there was an incident again a year later involving the same offender he had just reported it to Playstation and hadn't bothered with the police or Action Fraud. As Alex noted in relation to Action Fraud:

I got a reply but it was an annoying reply. Action Fraud actually recommended that I dial 101, which is basically they've told me to contact the police, and it's like well, I did that and they told me to contact you guys. Alex [Hacking, individual].

Lily had received a scam extortion mail which claimed there was malware on her computer, which Action Fraud had rejected as a crime and so when she did discover extensive malware on her computer she didn't bother reporting:

I didn't report them to Action Fraud because they didn't do anything the first time I tried to report the incident so I didn't believe that they would do anything. Also, the anti virus removes all threats so the problem was dealt with. Lily (Computer Virus, individual)

The police are unlikely to do anything because they are too busy

Some victims thought the police were very busy dealing with more serious crime and thought it would be unlikely they would be able to do anything. Perceptions of police capacity as being low in this area were a common theme in the interviews and a perception they do not have much in this area in terms of both resources and capability (this issue will be developed in more depth later).

Purely because I thought I was one of so many victims that... a) it was known about, because it was being talked about on various websites and news reports and what have you, and I didn't think I was going to get any response worthy of my time in reporting it really. Steve [Ransomware, SME].

Jackie, who was a serving police officer, also highlighted this reason:

Thing is, I know how limited that would get...I mean, certainly from a local force, there's limited that would get done and I'm aware that...I mean, Action Fraud, yes, but yeah, I'm very time poor at the moment – well, especially at the time of it happening [inaudible 04:12] building works and got two young kids so, yeah, I didn't...it took up more of my time which I didn't really have. Now I'm a bit more flush for time but the moment has passed. Jackie. [Hacking, individual].

Wrongly advised it was not a crime

Some victims did try to report, but were advised it was not a crime. Husksy, whose laptop was hacked by her estranged husband was told it was not a crime:

And he [the police officer] said, you are married, so if you leave it [the laptop] on the table, he's got access. But obviously there was a big misunderstanding, because it doesn't matter where I leave my computer, the point is that when I am online, I could be in a different country, but if I'm online, he can see that I'm online, and he can see what I'm doing, what I'm not doing. Husky [Hacking, individual].

Sam who had experienced her laptop being hacked used to take pictures of her and then threatened with public exposure unless she paid a ransom was also wrongly advised it was not a crime:

I was informed that there was nothing I could do. Apart from block the emails, cover my webcam and not part with money.

She went on:

...I tried printing them out and taking them in, but they just kind of disregarded what I was trying to say. It was almost like they were thinking, oh, this is just a friend who's being funny. But I'm like, no, this is actually someone who I don't know who's causing me real problems. And even if it was a friend, that's still not right. Sam. [Hacking, individual].

Never heard of Action Fraud

The interviews also highlighted the recurring theme of lack of knowledge of Action Fraud:

I have no idea what Action Fraud even is. Vanessa [Computer virus, individual].

I didn't know them. Nigel. [Ransomware, SME].

(heard of Action Fraud) No, I haven't. Gweneth. [Computer virus, Individual].

I didn't really know about Action Fraud at the time. I wasn't really aware of it. I didn't think it was serious enough for the police, I didn't want to bother the police with it. Charlie [Hacking, individual].

I didn't know Action Fraud was a thing, until you just said it. So, there's a problem. I don't know it's there. Sabrina. [Hacking, SME].

Another reason linked to this cited was that victims did not realise Action Fraud dealt with cybercrime:

I didn't really consider it a fraud. I'm aware now, obviously, that Action Fraud deals with cyber, like, computer misuse stuff, but I think the name Action Fraud is a bit misleading. James [Hacking, individual].

Embarrassment and fear of the consequences of reporting

Embarrassment and fear of the consequences of reporting was noted by a very small number of victims:

Maybe I was too embarrassed to report it, you don't know. Harold [Hacking, individual].

For one victim the reason for non-reporting (later when she realised initial advice was wrong) was the fear of the consequences of reporting because the offender was her ex-husband and the possible conviction might further impact upon her children, who had already been hurt by the divorce:

I am, and not only for that, my consideration is now, I have two almost adult children, and if my actions are actually going to be looked at, and their father gets some sort of attention, I need to consider the consequences on them. Because they already had quite a hard time during the divorce, 'cause he was really horrible. And what could be the results, and what could be the commotion of it? I don't think they want more attention, whether it is from the police, or from any other legal sort of body around, I don't know, I can always make an enquiry, if they don't have all my details, there is so much they can do. Husky [Hacking, Individual].

Jing was also concerned if she reported the incident that she may lose her laptop for a period of time which was crucial to her studies:

Yeah. I did, I [inaudible 0:06:50] because I'm not sure what were the [insurance 0:06:54] on my laptops because as student I need to finish up my dissertations and all that. So I might be worried that if they would take away my laptop, so I might have some difficulties in completing my research. Jing. [Computer Virus, Individual].

Another factor for Oliver was fear of potential consequences of drawing attention to himself as he was just about to emigrate to the USA:

Yeah, but this was around the time I was moving to the United States, I thought I don't want to draw attention to anything [inaudible 11:42], on their computer systems, given everything that had been going on in the press and whatnot. Yeah I [inaudible 11:55] as it was. I just put it down to [potential 11:59], virus that could have been on the computer that may well have just been laying dormant on the USB.

[Other factors discouraging reporting to the police/Action Fraud](#)

The interviews also provided leads to explore some other issues which also contributed to non-reporting by victims.

[Other websites where CMC is reported](#)

Many victims go to the service provider where the incident has occurred in the first place. Thus a person whose Facebook account is hacked, reports to them. An assessment was also undertaken by the authors of 39 websites where hacking is common, which showed many websites where initial reports might be made, yet do not mention Action Fraud or describe such behaviours as crimes. The assessment included banks, online gaming providers, social networking sites, email providers and online shopping providers. Only 4 of these specifically mention reporting to Action Fraud and in some of these it relates to fraud, rather than computer misuse offences. Most focus upon their own procedures for rectifying a hacked account, some offer further advice on prevention. Treating the incident as a crime or mentioning Action Fraud are rarely mentioned. However, it is important to note this was an assessment of the public reporting websites and providers, once receiving a report, may offer advice to report to the police or Action Fraud. Indeed the interviews revealed evidence of some victims being advised by such providers once they had reported to also report to Action Fraud. Nevertheless it would seem that many of the first places victim go to do not mention or encourage reporting the incident as a crime. Appendix 3 provides two examples of this.

[Action Fraud website](#)

A number of other factors were noted as discouraging the reporting of CMC to the police/Action Fraud were noted from the authors' assessments and some comments from victims. The name 'Action Fraud' is clearly a first barrier as it implies a website for fraud, not cyber- crime and this was an issue also noted by some victims. The authors' assessment also noted beneath Action Fraud on the main

website there is 'National Fraud & Cyber Crime Reporting Centre', but this is in very small font. Across the top of the website clicking on reporting reveals only report a fraud or phishing attempt with no mention of other cybercrimes. The A-Z of frauds covers some CMC offences, but unlike most fraud offences there is not a link at the bottom to report fraud. Overall the impression from the Action Fraud website is of one focused upon fraud, not the broader cybercrime offences. Appendix 4 illustrates these issues.

Police reporting websites

The interviews with victims suggested some confusion on who cybercrime should be reported to, with some been wrongly advised. One would expect victims who try to report to the police to be directed towards Action Fraud. The research team did not have the time to review all police websites, but a snapshot revealed some issues which may discourage reporting. Take the example of the West Yorkshire Police. The reporting page has no mention of any cybercrime (or fraud!). Clicking on reporting something else, also fails to lead to any links for cybercrime (or fraud). In another example from Surrey Police, the main reporting website mentions fraud (but does not direct to Action Fraud), yet not cybercrime. A better example of reporting was Dorset police, which more clearly illustrated where cybercrime should be reported on their website. See Appendix 5 for examples.

Reporting Experience of those Reporting to Bodies other than Police/Action Fraud

Among the survey respondents 56.7% (n=143) reported the incident to a body other than the police or Action Fraud. The most common body to report to, accounting for a quarter, was a bank or financial institution, followed by just under a fifth to a social networking site. Employers came in for 16.9% of reports, email providers 14.1% and internet providers 11.6%. Six of the interviewees had reported to such a body alone and there were a number of others who had reported to such a body and the police/Action Fraud.

Button et al (2011) found many fraud victims sent on a merry-go-round not knowing who to report to and sent from one agency to the next. Victims of computer misuse, particularly those who have had an account hacked generally have a clearer pathway to reporting. There were very few that started from a point of not knowing who to report to. Kathy who ran a small plumbing/central heating business with her husband had experienced a hack of her email where the offender had written to clients to notify them of a change of bank account for payments. She was unsure of what to do and so went to Citizen Advice and she was not impressed:

And she basically said it's your fault, it's your responsibility, you have to refund your client. So I was like, wow, I've just had my hands slapped. Kathy. [Hacking, SME].

However, Kathy was unusual as she did not know know who to report to. For some the only short inconvenience was contacting the police and then been told to go to Action Fraud. Before that stage, however, for most hacking victims the first organisation they consider – if they are going to report – is the relevant service provider. For example a person who thinks their bank account has been hacked, contacts the bank; an individual whose Facebook account has been compromised contacts them. For computer virus and ransomware victims there is not always a service provider or employer that has any responsibility for the device, meaning there is no body to report to other than police or Action Fraud.

As was noted earlier the information provided by such service providers does vary, with some not providing a clear website page identifying what the victim should do. Some only offer online means of

reporting, when the victim might prefer to talk to someone. The first challenge for victims is therefore to find the relevant guidance on how to report the incident and what to do. The nature of the victimisation means some victims prefer to want to speak to someone, but often the initial reporting mechanisms do not allow for that. For example, Ann experienced challenges with eBay:

Not that easy really; trying to find out how you kind of went about it. I think we were going through two or three different sites and she was saying, well, maybe, you know, this is where we need to go. And I think that's why we tried to get in contact with eBay, but obviously that's quite a hard thing to do in itself. Ann. [Hacking, Individual].

The victims who had experienced a hack of their bank account were generally all very positive about their reporting experience to banks. They could contact by telephone in a reasonable period of time, their issue was dealt with and they were also usually offered instant advice on dealing with the situation and enhancing their security.

Yes, they couldn't be more helpful, understanding. I mean, I was feeling such a prat at the time, but they were kind, considerate, got straight on with it. Told me what they had done, what I now had to do and what the process would be to reopen the accounts again. Henry. [Hacking, Individual].

The experience of victims relating to organisations other than banks, however, was much more mixed, with more negative experiences:

Then around PayPal, PayPal were useless because they said they couldn't see the transactions. They just seen it's been done as a guest. Catherine. [Hacking, Individual].

Facebook have been useless. Catherine. [Hacking, Individual].

Some did experience positive outcomes, however:

Well, they...I suppose they did their job at the end of the day in getting me the money back on it, but I think they really just kind of like passed me onto somebody else. Ann. [Hacking, Individual].

I realised what was going on. I immediately phoned up the customer service department at Apple, who were absolutely fantastic. They passed me through to the fraud department with them, because as she didn't have my password they classed it as fraud. And we set up two forms of ID so only my phone and iPad actually link to my account now, and if anybody logs in I get a text message straight away and an email to say someone's attempting to log in, and it gives me a unique security number just for that incident so nobody else can actually get in. Yet – but I daresay there will be ways round it in the future. Leo [Hacking, individual].

[Experience of Victims whose cases were reported to the Police and/or Action Fraud](#)

Drawing on the interviews with victims and the survey of 252 victims the following section will illustrate their experience of reporting. It is also important to remember the caveats noted in section 3, particularly the methods used to identify the victims means they may not be representative of all victims. The victims who reported to the police and/or Action Fraud are listed in table 7.1 below and the means by which they reported identified.

Table 7.1. Victims' means of reporting to police and/or Action Fraud

Name of Victim	The Police	Action Fraud
Ralph	Telephone (999)	
Henry		Online
Nigel	In person (visit)	
Sabrina	Telephone (101)	
Peter		Online
Bernard	Telephone (101)	Telephone
Kathy	Online	Online
Hilda (Via Adrian)	Telephone (101)	Telephone
Ann		Telephone
Lizz		Could not recall
Alex	Telephone (101) (and police force where offender through to live)	Online
Claire	Telephone (101) (After Action Fraud)	Telephone
Justin		Online
Aliya		Online
Sophie	Telephone (poor recall)	Online (poor recall)
Cameron		Online
Caroline		Telephone
Catherine	Telephone (101)	Telephone
Husky	In person (police station)	
Terry	Telephone (101)	Telephone
Sarah	Telephone (101)	
Angeline		Website
Arnold	Telephone (poor recall, not certain)	
Godfrey		Website (poor recall, not certain)
Paul		Telephone
Natalie	NCA contacted her after report to bank	
Lily		Website
Joana		Website
Patricia	Multiple reports	Multiple reports
Wayne	Telephone (101)	Telephone
Benjamin	NCA contacted him after report to bank	
Mark	Telephone (101)	
Leo	In person	Website
Mathew		Telephone

Michael		Could not recall
Kate	Website	
Jerry		Telephone
Sam	Telephone (101), website and in person	
Authur	Contacts	Telephone
Kellie	Telephone (101)	

The victims provided a wide mix of means of contact covering both police and/or Action Fraud via the relevant websites, telephone and in person. Some of their experience is highlighted below.

Reporting experience of those reporting to the police

Victims of CMC offences should in most cases report to Action Fraud. The motivations of victims reporting to the police included not knowing about Action Fraud and thus going to the police in the first instance and been told to report to Action Fraud or directly transferred. Some victims also wanted to report to the police and Action Fraud. There is also the added complexity that some cybercrimes should be reported to the police in the first instance, such as those involving harassment.

The survey data found 29.8% (n=75) of victims reporting to the police and the most popular means been by telephoning 999³ (36% of police reports), followed by dialling 101 (22.7% of police reports), website (21.3%) and in person (18.7%). The survey found vis-à-vis police reporting, some of the following key findings:

- The police dealt with 9% (7) of cases as a matter of urgency;
- A total of 93% (70) of cases reported to the police were subsequently reported to Action Fraud, including 7% (5) that were urgent cases handled immediately by the police;
- 3% (2) were treated as urgent but were not reported to Action Fraud or any other body;
- 3% (2) were not taken seriously and not reported to Action Fraud or any other body; and
- 12% (9) of those who reported directly to the police received protection advice from the police, compared to 42% of those who reported through Action Fraud.

The survey also sought data from the victims rating their experience of dealing with the police. This revealed:

- Overall 67% of victims who reported to the police were satisfied (strongly or tend to agree) with the experience;
- But it could be improved as 33% were not positively satisfied and only 23% were very satisfied;
- The reporting process worked well enough for most victims, 69% finding it easy enough (strongly agree or tend to agree) to report crimes;
- But it could be improved as only 35% found it very easy;
- Most victims (65%) felt the police staff were knowledgeable;
- But there is room for improvement as 35% were not positive about the officers' knowledge and only 28% felt the police were very well informed;
- 69% of the victims felt more confident in the police following their experiences with the police;

³ 999 should only be used for reporting an emergency or crime in progress, not for typical cyber-crimes which have already occurred.

- But the confidence of 31% was not improved, and only 33% were much more confident
- Contact with the police has increased most (68%) victims' risk awareness;
- Most victims (68%) feel more equipped to protect themselves as a result of the support provided by the police; and
- However, this does not translate well into more protective routines and more cautious online practices.

Most victims reporting to the police described the process as a positive experience. There were, however, a few victims who described a negative experience. Husky and Sam were both wrongly advised they could not report the incident:

And he said, you are married, so if you leave it on the table, he's got access. But obviously there was a big misunderstanding, because it doesn't matter where I leave my computer, the point is that when I am online, I could be in a different country, but if I'm online, he can see that I'm online, and he can see what I'm doing, what I'm not doing. Husky. [Hacking, Individual].

Sam also experienced this in relation to her attempt to report someone hacking her webcam and attempting to blackmail her:

I know, my husband was more shocked being a retired police officer himself and still being involved with the RTC side of policing (fair to say he was not impressed) at first I spoke to 101 who told me to use their online forms to log a complaint, I did so and never heard back from them. I phoned again and was told someone would phone me back, again no phone call, for the third time my husband took me to the station and we spoke to someone on the desk. After what felt like a very brief discussion with an officer, I was informed that there was nothing I could do. Apart from block the emails, cover my webcam and not part with money. Sam. [Hacking, individual].

Patricia, whose case was very complex experienced many challenges because of multiple police forces been involved been passed from force to force:

And it really is luck of the draw. And some offences were being committed in different territories, and the disparity between different police forces is huge. So the Met deal with it one way, Kent Police barely dealt with it at all. Exeter Police were very good when it involved lawyers, and they were creating gay sexual images of our solicitors. And Exeter Police, the Devon Police were very, very good and they were very together. The Welsh Police were very together, Lancashire Police were together. The Met were pretty hopeless. Luton were okay up until a point... Patricia. [Multiple, Individual].

Experience of those Reporting to Action Fraud

The survey data found 48% (n=120) of respondents had reported to Action Fraud or someone had reported on their behalf. It also found just over three quarters found Action Fraud via the police or another organisation advising them. The survey found regarding their experience (see Appendix 3):

- Overall 68% of victims who reported to Action Fraud were satisfied (strongly or tend to agree) with the experience;
- But it could be improved as 32% were not positively satisfied and only 29% were very satisfied;

- The reporting process worked well enough for most victims, 80% finding it easy enough (strongly agree or tend to agree) to report crimes [better than the police];
- But it could be improved as only 37% found it very easy [same as police];
- Most victims (75%) felt the Action Fraud advisors were knowledgeable [a little better than the police];
- But there is room for improvement as 25% were not positive about the advisors' knowledge and only 33% felt the advisors were very well informed [a little better than the police];
- 70% of the victims felt more confident in the police following their experiences with Action Fraud [same as police];
- But the confidence of 30% was not improved, and only 30% were much more confident [same as police]; and
- Contact with Action Fraud has increased most (70%) victims' risk awareness [similar to police].

The interviews confirmed this as many of the victims at the point of victimisation had not heard of Action Fraud. Only via their own research, advice from another report receiving organisation or by going to the police first did many of the victims come to Action Fraud. As the section above illustrated and as this section will show the name and online information does not clearly direct victims of CM offences to Action Fraud, unless there is a fraud element to the offence:

I think it was one of the banks that said, well you need to use Action Fraud. That was it. Henry. [Hacking, Individual].

I don't remember if I had heard of it or I looked it up and found it. Action Fraud is, kind of, the branding of it. I don't know. I think I was aware that there was somewhere to report and so I did. Cameron. [Attempted Hacking, Individual].

I think I just looked it up on the internet, I put in spam emails, or something, and then it came up you should report to Action Fraud, but I don't know the proper procedure really of how to do it, I'm just, sort of, guessing. Peter. [Hacking, Individual].

Justin did some research to identify who to report to, but his management were still not convinced.

I remember a conversation with the assistant headteacher as well, who was my line manager at the time. So, she said, but it's not fraud. You know, this is who have been told to report it to. So, I think, yeah, perhaps the name is a bit misleading. Justin. [Hacking, SME].

Alex who had started with the police and was told to contact Action Fraud, was actually told to report to the police, when he did contact Action Fraud:

I got a reply but it was an annoying reply. Action Fraud actually recommended that I dial 101, which is basically they've told me to contact the police, and it's like well, I did that and they told me to contact you guys. Then I got no reply from my message saying... Alex. [Hacking, Individual].

The survey found 41% reported by the website and 39% by telephone. The experience from the interviews relating to the two forms of reporting will now be assessed.

Telephone line experience

Those reporting to Action Fraud via the telephone generally had a positive experience:

I think at the time I found it, you know, they were really helpful. They just asked the different bits, you know, that I told you. A minute probably would have been 20 minutes, half an hour, but it didn't worry me because I thought I'm telling them what happened. Caroline. [Hacking, Individual].

They were really good. They were probably on about...two hours on the phone to them. They were really good. Catherine. [Hacking, Individual].

They are very reassuring. I mean, when you feel...you feel you're talking to determined people but they're pretty helpless, actually. There isn't much they can do, I think. Bernard. [Hacking, Individual].

In terms of logging it, they were probably quite helpful, like...they didn't make any false promises or anything like that. You know, sometimes they might have said, like, oh we'll promise we get you? They didn't say any of that. They were just quite factual. In terms of what they actually told me, I can't remember word for word, what they said. Paul. [Hacking and Denial of Service Attack, Individual].

Authur, however, was critical of their knowledge:

They haven't got a clue. They're literally just call handlers. Authur. [Hacking, SME].

Website experience

The experience of reporting via the website was much more mixed with some positive, but some very negative. A number of negative experiences noted the process was such they were tempted to give up.⁴

It's pages and pages and pages of stuff that you're relevant to reporting what I had and it took forever. It took, I don't know how long, 45 minutes or something. Cameron. [Attempted Hacking, Individual].

Yeah, I used their website, and I filled the form in, I remember, it took quite a while; and then somebody contacted me, and I sent them all the communications. Aliya. [Ransomware, SME].

Action Fraud's website is awful as well. It felt like I was submitting to something from the 1990s. I don't know how they managed to make a website that looked so archaic. It takes some skill. It's incredible. Alex. [Hacking, Individual].

However, some victims were positive about the website reporting experience:

It was quite easy. I just had to state when it happened, what happened and I had to write a little paragraph about it and tell them any steps I had taken so far and stuff like that. It was quite easy. Lily. [Computer Virus, Individual].

⁴ The website has changed and most victims had reported under the old website.

Pretty easy to do. I'm actually dyslexic and their website I could manage it. My spelling was atrocious, don't get me wrong. But I did phone them up after I reported it and asked for their advice what to do and they told me to take it to the local police as well because I've actually got a confirmation address with one of the emails from Apple of where they'd logged in from. Leo. [Hacking, Individual].

Husky had not reported it, but had used the web chat facility, which she was positive about:

And I only recently, I have had this online, there is a chat facility on the Action Fraud website, and I just said, out of curiosity, is this considered a crime, because the police told me that it wasn't, and he said, no matter what is your relationship with a person, if you don't give permission for somebody to access your computer, it is illegal. He said, you need to send it in to us, to be considered, and then we'll decide whether to take action or not. Husky. [Hacking, Individual].

8. The Response of the Police/Action Fraud

Once a victim has successfully reported a case of CM one can imagine an ideal response for a victim might be: the immediate needs are satisfied relating to technical support, relevant guidance on prevention and dealing with the incident, emotional support etc. Information is provided on the progress of the case. That action is pursued to prevent more of these types of incidents. Most victims are also likely to want a police response involving an investigation, identification of an offender and successful prosecution. The latter given the size of the problem of this type of crime is very unlikely. The survey provided some interesting data on what support reporters to Action Fraud actually received.

Table 8.1. Survey data on what happened to victims who reported to Action Fraud

	Count (Yes)	% of victims reporting to Action Fraud
Received meaningful updates from either Action Fraud or the police regarding what was happening with my report	47	39.2%
Received regular updates from either Action Fraud or the police regarding what was happening with my report	40	33.3%
Received information via email or telephone on how to protect against becoming a victim of cybercrime again	35	29.2%
A police or community support officer visited me in person to provide information on how to protect against becoming a victim of cybercrime again	18	15.0%
Received information that a police investigation would not be happening	11	9.2%
Received information that a police investigation was	5	4.2%

being made into the incident		
Received information on the final outcome of the police investigation	8	6.7%
Advised that the incident would be recorded by a financial institution and no further action required	8	6.7%
Advised that the incident was not being recorded as a crime	7	5.8%
Other [please specify]	1	0.8%
None of the above	2	1.7%
Tot	182	151.7%
n	120	

Some of the key findings from this table illustrates are as follows. Of those victims who reported to Action Fraud (n=120):

- Less than 40% (47) felt they received meaningful updates about what was happening with their report;
- Only about 1/3rd (40) received regular updates or advice about protection from Action Fraud about what was happening with their report ;
- Only 15% (18) of those reporting to Action Fraud were visited by the police service;
- Only 7% received a report on the final police outcome;
- Overall 42% (50) received protection advice as a result of their Action Fraud report, compared to 12% of those who reported only to the police;
- 29% (35) received advice by email or telephone about how to protect against becoming a victim of cyber crime again;
- 15% (18) subsequently received advice from a police or community support officer; and
- 3% (3) received advice through both routes.

Some of these issues will now be developed in more depth using the interview data along with some other related issues that arose from it.

Disappointment at Action Fraud classification

Some victims are disappointed at the classification of their incident not as a crime. For Aliya her case was classified as civil, which she could not understand:

They said civil, this is a civil case; and I said, okay, I mean I already did that. But I mean why must one go and do that instead of stopping the perpetrator; I just felt that the person who was dealing with my case wasn't experienced in the online world, and they couldn't understand the consequences of letting someone like that loose on the public and making lots of money feeding off people. Aliya. [Ransomware, SME].

Lily was also disappointed:

They emailed me back saying that they was closing the case. They weren't going to investigate the case because apparently it wasn't a crime. Lily. [Computer Virus, Individual].

This made her:

Like, disheartened 'cause I think it is a crime. Lily. [Computer Virus, Individual].

Frustration at perceived lack of action

For most of the victims who did report to Action Fraud/Police the case was accepted. However, for some of these there was a perceived lack of action.

Lack of any response

For Henry, he had not even received an email or letter from Action Fraud after reporting the incident, relating to his case. Bernard could not recall if he had, but his memory was not brilliant:

No, I don't remember. Gosh, I'm sorry I just can't remember whether I got a letter. Bernard. [Hacking, Individual].

Ann could also not recall:

I don't remember getting a letter, I may have got an email from them just saying, you know, that they were dealing with it, but I don't remember getting a letter at all. Ann. [Hacking, Individual].

Response to say no further action

Most victims who reported, however, did receive a letter/email, but stating there will be no further action relating to the case. Kathy also commented on this:

Yes. I still did it [report to Action Fraud] straight away. I didn't get any help from anybody. They basically said, you know, great, thanks for letting us know and we'll look into it. And that was it. I didn't know if they meant they'd look into our case or, you know, it's something we're looking into. Kathy. [Hacking, SME].

Lack of information on progress of the case

Some victims were frustrated at not hearing information on any progress in their case. Caroline felt there should be more information on the progress of the case provided:

I thought it would have been nice to hear a bit more but, you know, they probably could have just traced it to them, it's a dead end. I always think it's always nice to hear an outcome or follow up of something. Caroline. [Hacking, Individual].

Advice and support received from police/Action Fraud

The reporting victims in general did not receive extensive support and advice as a result of their report. A tiny number experienced an investigation. There was little evidence of advice on the prevention of future cybercrimes been provided and many of the victims remembering or taking note of it. There was also evidence that the information received was the very basic.

Information/advice from Action Fraud

Most victims interviewed who reported to Action Fraud did not recall receiving any or very much support if their case resulted in no police interest. Victims received letters and emails (with links to further advice) which most did not pursue, note or remember. Cameron noted he had received such emails from Action Fraud, but the nature of them led him to delete them. The official classification of the correspondence also seems to confuse the victim:

In September I got an email that I'm looking at, at the moment, it says Action Fraud and Lloyd's Bank ask for your assistance to help prevent cybercrime, not protectively marked. Classification in red, not protectively marked. Dear sir/madam, and then a bunch of stuff, so naturally it says not protectively marked which means ignore this. Whether it's valid or not, I don't know. But if that comes from AF victim contact, City of London, PNN Police UK, that's scary, not protectively marked. Cameron. [Attempted Hacking, Individual].

Kathy did not recall any support:

I didn't get any support and certainly no updates. It was basically thanks, we'll look into it. Kathy. [Hacking, SME].

Justin received an acknowledgement and no further advice or support.

But I'm fairly sure it was just an acknowledgement. I don't remember ever speaking to anyone before I spoke to the police officer who said, they weren't taking any action. Yes, this is the fraud confirmation. Justin. [Hacking, SMO].

Terry could not recall receiving any specific support, although he did look at the Action Fraud website, which he found useful and he did get regular emails from them:

I get emails occasionally, yeah... Terry. [Computer virus, Individual].

Angeline received an email a few months later:

About six months later, I got an email. I'm sorry, it's coming back to me as we speak. Yeah, I got an email about six months later telling me, basically, that there was no action that could be taken and explaining... If I could find the email... Angeline. [Hacking, individual].

Paul received basic correspondence but noted he had been advised action was unlikely:

I think it was open for a while, and then I think I received correspondence saying that there wasn't enough evidence, so there was nothing to investigate. Paul. [Hacking and denial of service attack, individual].

Claire compared the support she received from Barclays, which she thought was better than Action Fraud:

I think it was Barclays that did more. They gave me a couple of helplines, support and that, and I think it must have been through Barclays that I heard about what you were doing at the university and that. I'm sure it was Barclays. Claire. [Hacking, Individual].

Some victims, however, did note some positive advice from Action Fraud. Adrian who was the son of Hilda noted:

Well, I think the advice was to create an account or get me or my sister or someone to look after it and perhaps, well they definitely gave her the right advice like, don't do this on the phone, don't say this, no one is ever going to ask you for your details on the phone. I kind of think she already knew that but she was going through a bit of a...I don't know. My granddad had just died, her dad, so she was not happy, you know. Adrian. [Son of Hilda, Hacking, Individual].

Several victims were also confused by what Action Fraud actually is thinking it is specialist police unit dedicated to investigating fraud, rather than a reporting centre. Joana thought she got a letter from the fraud squad when it was Action Fraud. Some thought they were actually communicating with fraud squad police officers at Action Fraud.

[Awareness of sources for advice/support to prevent victimisation](#)

There are a wide range of websites offering support that are either run by official bodies or have the endorsement of them. Figure 8.1 lists some of the main websites identified during this research relevant to the UK.

Figure 8.1. Websites offering advice and support in relation to computer misuse offences⁵

Name of Website	URL	Description	Recognition among victims
Action Fraud	https://www.actionfraud.police.uk/	Official reporting website, with description of different types of CM crime and general prevention advice	Medium
Getsafeonline	https://www.getsafeonline.org/	Extensive advice on different types of CM crime with specific advice	Low
Take five to stop fraud	https://takefive-stopfraud.org.uk/	Fraud prevention advice with some overlap with CM crime	Low
National Cyber Security Centre	https://www.ncsc.gov.uk/	Extensive advice for individuals, SME/O on prevention of different types of CM offences	Low
Havebeenpwned	https://haveibeenpwned.com/	Website where a person can check if an account has been compromised	Very low
Nomoreransom	https://www.nomoreransom.org/en/about-the-project.html	Website offering advice on tackling ransomware	Very low

Note:

1. Cyberaware now leads direct to National Cyber Security Centre and has been excluded from above, but was treated separately in survey.

A significant finding was that not only did most victims have little awareness of these websites both before the incident, but after the incident too. One would expect those who have been victims to seek more information on prevention and those reporting to receive such information. The survey data and interview data did not provide evidence to support the positive change one would expect (to be discussed later). These show for:

⁵ Other websites found which offered good advice, not listed in figure 8.1 above:

- Very good advice on preventing and dealing with CM offences from a relationship, domestic abuse and stalking type perspective <https://www.refuge.org.uk/our-work/forms-of-violence-and-abuse/tech-abuse-2/resources/>
- Another related to domestic abuse from the USA <https://hackblossom.org/domestic-violence/>
- Victim Support has some general advice <https://www.victimsupport.org.uk/crime-info/types-crime/cyber-crime>

- Action Fraud
 - 24.6% very aware before, 34.1% after
 - 31.3% unaware before, 17.9% after
- Getsafeonline
 - 17.5% very aware before, 25.4% after
 - 45.6% unaware before, 34.9% after
- National Cyber Security Centre
 - 19.8% very aware before 27.4% after
 - 37.7% unaware before, 27.8% after
- Take five to stop fraud
 - 15.1% very aware before, 22.2% after
 - 49.6% unaware before, 36.1% after

For these main websites there is a positive movement in terms of awareness after the incident, but still not brilliant. Action Fraud as the reporting body and most prominent website only has just over a third of respondents very aware of after the incident and almost a fifth unaware. This finding was also found in the interviews with victims. It closely relates to a finding of the lack of changes in security behaviours of some victims as a result of the incident. Justin, who was responsible for cyber security in his school could not identify any:

Not on the top of my head. No. Justin. [Hacking, SMO].

Others also fell into this category:

I haven't look at any of those. Catherine. [Hacking, Individual].

I've just never heard of them. Angeline. [Hacking, Individual].

Jackie, who was a police officer, had only heard of Action Fraud:

...even in the police I've not been told of any other one. Jackie. [Hacking, individual].

Oliver was also only aware of Action Fraud:

I know...I'm trying to think, is it...I'm sure Action Fraud has something within their website, when I'm doing research for something to do with work. I use their website as a sort of go to for information. But I mean other than the software security companies that's the only one I can think of. Oliver. [Computer virus, hacking].

Some, however, did think if they needed specific advice they could find it:

Not specific ones, but if I needed advice, I know that I could just google it. Paul. [Hacking and Denial of Service, Individual].

I wasn't aware of any but I guess you could just google some and it'll come up. But not off the top of my head. Lilt. [Computer virus, individual].

No, I mean, no, I mean you know I suppose, if I was looking for it, I'd just google in whatever it is I want, yeah. Benjamin. [Hacking, individual].

An issue for some victims was determining if a website was genuine or legitimate.

I'm aware of a couple but then they look a bit dodgy so I'm like, because you don't know what's real, what's dodgy these days. Ralph. [Ransomware, SME].

Not all victims behaved this way and there was some evidence of victims using advice found from suggested websites or searching for advice and support themselves. Steve had made use of the website nomoreransom to help deal with his incident. Lily had googled for ideas of support and how to deal with the incident.

[Visit or contact from the police to take a statement or provide support](#)

A small number of victims received a telephone call from the police, others a visit. In Sabrina's case because of the possible hacking by a terrorist group of her website she received both a call and a visit from the police. However, she commented:

I didn't get any sense of his knowledge level on cyber security or hacking in particular, he was really concerned with taking information from me, and getting everything I knew, and everything that we'd experienced. Sabrina. [Hacking, SME].

However, following the visit she felt it was a logging process with little intervention to try and prevent such incidents occurring again.

It was efficient, but my perception of the situation was it was really a logging process, and I didn't know what was going to happen then, for them. I certainly felt like we'd been taken seriously, that an officer had come out to speak to me. But there was no follow up process, in terms of, can we talk to you about...given that we're a journalism organisation, could we talk to you about maybe improving your cyber security, or having an awareness, or anything like that. There was nothing like that, but everybody I dealt with was professional, but as I say, the perception I came away with was really, it was a log-in process...and it was no real concern of mine, from their point of view, what happened afterwards. Sabrina. [Hacking, SME].

Two victims actually identified leads they felt could locate the offender (the reality might have been different), but were frustrated at the police response to this information. Alex had actually done his own research to try and identify the offender and wanted to give this to the police to help their investigation, but was disappointed with their lack of interest:

The response was disappointing. I wanted to basically hand over the information I had which I thought might be of benefit, if they know that an address is associated with hacking then if that popped up again they could use it, or they could just knock on his door. That's also an option, especially because one of the photos... So as part of this, and it kind of like encourages somewhat defensive and paranoid behaviour, so of all the different accounts that he was using I was scrolling to see if there was anything I could use to defend myself in the future. So one of the things I was able to find was what looked like a photograph, some sort of selfie, and so that's in my folder of information that maybe this person...and a whole bunch of some of the names that he seemed to be using, especially the older ones before he adopted nicknames and stuff. So I did a little bit of snooping just so I had something to fall back on.

And I thought it was reasonable and potentially valuable for the police to have that as a resource of...not necessarily evidence, but certainly associated. Alex. [Hacking, Individual].

Jerry had also identified the offender's address and was disappointed there was no interest:

At that point, I phoned Action Fraud and explained to them, and gave them the details. And they said, well, there's probably not a lot we can do. At which point, I said, well, do you want their address? Because I'd logged into my Ali Express account and changed the password straightaway, and they hadn't had a chance to remove their address from the delivery details as yet. So I had the name, the address and the phone number for the person who it was being delivered to, in Manchester. Jerry. [Hacking, individual].

Some victims did receive extensive support. For Catherine, however, she had experienced regular contact and advice from the police. They had taken a statement from her and the officer kept in regular contact updating her on the case and giving her advice:

He's messaged most days really. So he left another message today. He's either emailed or phoned. He's sent loads of long emails with lots of different links and other things and suggesting I should do passport manager and other things. Catherine. [Hacking, Individual].

Claire in addition to reporting to Action Fraud, even though they advised her not to, also contacted the police because she was very worried and low at that point. She received a referral to Victim Support from them, which she contacted:

[the police] Just quite supportive on the phone and that, and then they gave me another helpline number and it was like a victim support thing. And I did call it and, I don't know, I think it made me worse. I just sat on this phone crying to this lady, but I was still in shock then, I think, and I couldn't believe I'd lost all my money and we were panicking about the mortgage and the house and everything and what were we going to do?

Several SMEs received a visit or contact from the police once reported, but felt the police lacked expertise and the capability to deal with such crime. Mark received a visit from a police officer:

Yeah, he did say, look I don't think this is...we're going to get much out of this, you know, we'll keep a record of it and if...it might help in other cases and similarity of other cases. But whether we actually solve the case or, you know, bring anybody to justice for it, I doubt, you know, that's what he said, that was it but he, certainly in terms of his technical ability, was very limited. 'Cause, I said to him, I can remember saying to him, I think...'cause he said, how do you think they got in? I said, I don't know, if I knew I would, you know. 'Cause it's a secure thing, I said, but from one of the files on the logs that I...it looked like it came from an IP address which is not known to me. And, when I did a trace on that it goes to somewhere in Eastern Europe, I said, and that's as far as I've got. And, he didn't understand that. And, he didn't understand where the various files were, so his IT skills were very limited. Mark [Ransomware, SME].

Mathew, also experienced a police response that showed limited capability:

We sent off all the investigation results and the reports to him and he probably came back to us, I would say, within about three weeks approximately, something like that, just to say that there's nothing we can do really about it. Yeah, it's too difficult to trace, yeah. Mathew. [Hacking, SME].

Authur experienced a police visit (staff and officers) which exposed their lack of knowledge and resources:

One of the lads that came down here... The initial bobbies that come down, they said, right, we're going to send someone to copy your hard drives. I said, bearing in mind, it's 4 or 5 terabytes you need to copy, they said, yeah. The police cybercrimes unit don't have all of these police officers; they employ some of the lads fresh out of uni. As you work in a uni, a piece of paper means absolutely rat shit...

He went on:

So he [police IT specialist] comes down, he sits where you're sat, and he gets this docking station out. See, this...it's a £4.99 docking station for hard drives off eBay. I said, I binned them about five years ago 'cause they're crap, they're outdated. Oh, no, no, [this will work 20:35], so he plugs it in and starts copying it across. He asks me a load of questions for about an hour and he says, well this is going to take all weekend, this. I said, I did tell you that. Well, ooh, oh... I said, just take the hard drive with you.

The knowledge of the police IT specialist were further exposed:

Now, there was another bobby with him who was an actual copper, sat with him, who knew nothing about computers whatsoever and he admit it. He was just coming with him. He was doing the questions when he was doing the IT. I said, just take the hard drives with you. So he starts picking up the laptop and the copper is shaking his head, it's the hard drives. So this is the computer guy who's looking, well what do you mean, will I take the hard drive out the laptop? I said, the hard drive that you're copying across that are right next to the laptop, take it with you. Huh, hey, what? So the bobby who knew nothing about IT had to show him what the hard drive was to take with him. Authur. [Hacking, SME].

Experience of police investigation

Some victims did experience some evidence there was a police investigation, but it did not lead to anything:

I then got a response off the police, saying, nothing was going to happen, there wasn't enough evidence or whatever. But then a few months later, or this might have been last year, I got an email off someone from Action Fraud, saying that they'd re-opened it, 'cause they'd had more evidence, and they wanted me to answer some questions. Paul. [Hacking and Denial of Service Attack, Individual].

This, however, did not lead to any success in bringing to justice the perpetrators. Arnold received a visit from the police on the day of the report:

They were excellent, they came in, I think, later that afternoon they were in. They actually came in in person, they sat down, we laid out exactly what had happened, they obviously advised us don't pay anything. Arnold. [Ransomware, SME].

They received further contact:

They...if I remember correctly, they contacted us about a week later to know if we'd...you know, just to follow up saying is all of our data 100 per cent okay, have we heard anything further from them. Arnold. [Ransomware, SME].

And then further contact:

...gave us an update just to say, look, they hadn't managed to decrypt the files but they were looking into it because... And we had a brief chat about the whole NHS situation and the fact that that had gone on but that was it, that was the sum total. I think because there was no damages, there was no insurance claim, there was no...it just became a fairly low priority, you know. Arnold. [Ransomware, SME].

Leo experienced informal help, where the police visited his estranged wife and warned her not engage in such behaviour:

The officer I spoke to at Humberside he was fantastic. I handed the form to him but he was perfectly honest, he says, we might have the address, we know who did it, but it's a choice of three people: my wife, my stepson or his partner. Because they were all living in the same address. It's a case to prove who actually did it, that's the difficult part. But he said he would go and have a word with them, warn them off the record if it happens again the police would be taking action. But he was totally straight with me, he said there's no way the CPS would take it into prosecution, but if it keeps happening then you would have a case of harassment. Leo. [Hacking, Individual].

We went on:

No, they just said they'd spoken to them and it shouldn't happen again. Leo. [Hacking, Individual].

Only Sophie, Sarah, Natalie, Benjamin and Mary experienced a successful police (or NCA) investigation resulting in a judicial outcome. Mary's organisation received police interest when the case reached the media, but not initially. Sophie made her report via the telephone to Action Fraud and two weeks later she received contact from the police when a visit was arranged to take her statement. She was happy with the process and received regular updates as the case progressed:

[Updates on case] I did, through the process. I mean, he would certainly keep me updated with any new information. Sophie. [Hacking, Individual].

She also received advice from the police on enhancing her security:

And that was one of the things...I mean, I always thought it was anyway. But, after that, obviously the first thing that the police say to you is, you must make sure that you change everything, and step up your security settings, et cetera, et cetera, so obviously you do. So, I'm far more aware of that sort of thing now, than I ever was. Sophie. [Hacking, Individual].

The case resulted in a police caution for the offender. However, Sophie was not happy with this and had wanted it to go to court and for a tougher sanction to be applied.

I just wish the outcome had been a stronger outcome in my favour. I think that he got off too lightly, considering that he tried to ruin mine and my family's future. Yeah, I would have had

my day in court, if I'd have had my way. And unfortunately that opportunity wasn't given to me. I'd have shut him down. I'd have stopped him from trading, which is something that could have happened, that could have been an outcome. Sophie. [Hacking, Individual].

Sarah also experienced a police investigation, but which also involved the National Crime Agency in relation to a financial investigation of the offenders.

I think they [Action Fraud] were very good, having spoken to somebody on the phone, they then asked, would I be willing to make a statement, and a policewoman would come and take that statement. And, in fact, one did, she came, she identified herself, she come from, I think it was Hexham Police Station, and ended up in Northumberland, and she took my statement. I said, I've written one out and she said we need to do it from scratch. So, she did and I signed it and she went off. And, it was then, they said they would investigate and keep me informed. And, the next I think that I knew was that I got a letter from [name of team] Criminal Finance Team based in Bristol.. Sarah [Hacking, Individual].

She was very happy with the police and NCA who regularly kept her updated throughout the case. She was also asked if she would be willing to go to court, which she agreed, but did not have to. The case resulted in the offenders been found guilty and assets confiscated. She commented:

I thought it was very good the support that I got from them and to get the updates and would I be willing to be a witness, if necessary, and I said, yes, I would. But in fact, that proved not to be necessary, which in a sense was quite good, quite a relief. Sarah [Hacking, Individual].

Natalie's case also resulted in a successful case of conviction arising from an NCA investigation. She compared the response of the NCA dealing with the hacking incident to the local police when burgled:

[The NCA] Very good, as far as I was concerned. I'd never come across them before, at all, but they certainly rang up periodically, and kept me informed and told me what was going on, which is entirely different from the various burglaries that we've had over time... [where no police response]. Natalie. [Hacking, SME].

She also felt they kept her well informed throughout the case:

And the National Crime Agency have been very good. They ring me up about every four, six months, something like that and said, it's going to court in March, no, it's been postponed or whatever, they've just kept me up to date. And then they rang me a month or six weeks ago, something like that, not a huge amount of time ago, to say that some people had been convicted, and it was one of a number of frauds that they'd been prosecuted for. Natalie. [Hacking, SME].

Benjamin experienced a successful investigation from the NCA and he had only reported to the bank, so was surprised when they contacted him and then embarked upon a successful investigation:

Well, I suppose, my reaction when...because I had a couple of phone calls from, and I think it was the NCA, plus a visit from somebody from the NCA, and then there was about four letters that came in over the last year, two from one agency, two from the other. And, they were letting me know, I suppose, that the crime was being followed up, you know, right the way to the point when the trial was due, and then the outcome of the trial. So, I suppose, I was quite grateful really to be kept in touch with that. Benjamin. [Hacking, Individual].

Survey victims' views overall on Action Fraud, the police and other organisations compared

The survey sought general data on the views of victims on Action Fraud and the police overall. The table 8.2 below provide a comparison between the police, Action Fraud and other organisations victims report to (such as banks, Facebook etc). Generally the scores are similar with some slight differences (it must be remembered the nature of the survey was such it cannot be considered representative of the general population):

- Ease of reporting Action Fraud is slightly better than police and other, with other marginally better than the police.
- The staff spoken to were well informed, Action Fraud also came out slightly better than other with the police behind both.
- In terms of awareness as a result of contact, the police scored highest with other and Action Fraud very similar.
- In terms of support to better equip the victim all three were very similar in score in terms of strongly agree/tend to agree, but Action Fraud scored significantly lower on the strongly agree.
- Both the police and Action Fraud scored similarly on the response inspiring confidence in the police.
- However, in terms of overall satisfaction with reporting other organisations scored slightly better than Action Fraud, followed by the police.

Table 8.2 Survey victims' overall views compared on Action Fraud, the police and other organisations

		Action Fraud	Police	Other
I found it very easy to report the incident	Strongly agree	36.7%	34.7%	37.8%
	Tend to agree	43.3%	34.7%	37.1%
	Neither agree nor disagree	10.8%	18.7%	14.7%
	Tend to disagree	7.5%	6.7%	8.4%
	Strongly disagree	0.8%	5.3%	2.1%
	Don't know	0.8%	0.0%	0.0%
The advisors/police/other I communicated with were well informed	Strongly agree	32.5%	28.0%	32.2%
	Tend to agree	42.5%	37.3%	39.2%
	Neither agree nor disagree	15.8%	24.0%	20.3%
	Tend to disagree	5.0%	8.0%	6.3%

	Strongly disagree	4.2%	2.7%	2.1%
	Don't know	0.0%	0.0%	0.0%
I am more aware about potential cybercrime as a result of contact I received from Action Fraud/police/other body	Strongly agree	34.2%	32.0%	35.0%
	Tend to agree	35.8%	42.7%	33.6%
	Neither agree nor disagree	18.3%	17.3%	20.3%
	Tend to disagree	10.0%	6.7%	6.3%
	Strongly disagree	1.7%	1.3%	4.9%
	Don't know	0.0%	0.0%	0.0%
The support I received from Action Fraud/police/other made me feel better equipped to protect myself from cybercrime	Strongly agree	25.0%	36.0%	33.6%
	Tend to agree	42.5%	32.0%	35.0%
	Neither agree nor disagree	21.7%	16.0%	18.9%
	Tend to disagree	7.5%	12.0%	9.1%
	Strongly disagree	3.3%	4.0%	3.5%
	Don't know	0.0%	0.0%	0.0%
The response I received from Action Fraud/police has increased my confidence in the police's ability to respond to cybercrime	Strongly agree	30.0%	33.3%	
	Tend to agree	40.0%	36.0%	
	Neither agree nor disagree	17.5%	18.7%	
	Tend to disagree	10.0%	8.0%	
	Strongly disagree	2.5%	2.7%	
	Don't know	0.0%	1.3%	
Overall, I was satisfied with the experience of reporting to Action	Strongly agree	29.2%	22.7%	32.2%

Fraud/police/other body				
	Tend to agree	39.2%	44.0%	37.1%
	Neither agree nor disagree	18.3%	20.0%	19.6%
	Tend to disagree	9.2%	9.3%	7.7%
	Strongly disagree	3.3%	4.0%	3.5%
	Don't know	0.8%	0.0%	0.0%

9. Victims' Needs

Both the survey and interviews explored what support the victims wanted and what they actually received. The table shows that the survey victims saw all types of support as important. It also shows there is a clear gap between what they actually received and wanted. Immediate, technical and information were all rated as important by around three quarters or more respondents to the survey, but only a quarter received immediate support and less than a fifth technical support. The most common support received was information, but still only a third received this. The section above on the police Action Fraud response also illustrated many victims not receiving many of the types of support listed in table 9.1.

Table 9.1. Comparing what support victims wanted to what they actually received

Type of support	Support wanted rated very important	Support wanted rated Important (very or fairly)	What support victims actually received
Immediate support – where to go and who to talk to	39.2%	82.0%	25.80%
Technical support	37.6%	76.2%	19.00%
Information support	34.9%	74.6%	33.30%

Emotional support	30.2%	64.0%	12.30%
Financial support	40.2%	63.5%	6.00%
Practical support, bureaucracy	35.4%	60.3%	6.30%
Formal counselling/therapy	30.2%	59.8%	6.70%
Advocacy support	33.3%	55.0%	3.20%

The interviews identified a number of key areas that victims identified as what they wanted in terms of support.

Information about the case and what happened

Many of the victims interviewed did not know exactly what had happened, who had perpetrated the attack and what the authorities were going to do. This basic information was central to what many of the victims wanted:

Well, really, nobody. I mean, I did feel a little bit at the time like...that I wanted somebody to come back to me to tell me what had happened, but nobody did, they just sort of said... Ann. [Hacking, Individual].

Or, not even if, 'cause obviously, yeah, people don't always get caught do they? But even just to know what they'd done, or what had happened, what they'd maybe explored, and you know, that information might be available, if I contacted them and said, excuse me, can you give me all the information? But whether they would, I don't know. It would be nice to sort of know what's happened behind the scenes. Paul. [Hacking and Denial of Service Attack].

It would have been good to know that the police could have done something. I guess leaving it open-ended, saying, yeah, we just can't trace these people, I guess that makes you feel slightly insecure online. And how the person got my Facebook password as well, because I'm assuming somebody would have had to log in as me, and that was a worrying thing. Angeline. [Hacking, Individual].

Technical support

The most important support victims wanted was technical support. This related to immediate technical support to rectify their situation, support to provide reassurance such an incident would not happen again and longer term preventative support. Several of the victims had sought technical support via friends/family, a specialist contractor or stores such as PC World. This type of support as some of the following quotes from interviews was the most clear type of support they wanted. Jing wanted one simple thing:

Make my computer work. Jing. [Computer Virus, Individual]

Nigel similarly wanted such support to restore lost files:

It's then having the specialist to be able to do it I suppose. They could I suppose if I was, there's my hard drive, take it away and solve it like that. Nigel. [Ransomware, SME].

Gweneth also wanted such support.

Practical, yeah, I think that would be useful just so the IT department, or whoever's relevant, can go through how to deal with this process and what's the best course of action should it happen to you. Gweneth. [Computer Virus, Individual].

As did Oliver:

Yeah, technical support. Because I don't think everyone's PC savvy to be totally honest. Oliver. [Computer virus, individual].

Lily wanted specific advice on what is good anti-virus protection:

Yeah, that would have been good because there's so many anti-viruses which say all different things, so I wasn't sure which one to get and which was more secure and stuff like that. So yeah, that would have been handy. Lily. [Computer Virus, Individual].

Catherine who had been hacked wanted specific advice on a password manager (which in her case was a rare example of a police officer who was actually helping her to do this):

Just about the password manager and other safety things that...No, just more information about how to move forward from it and not let it happen again, really. Catherine. [Hacking, Individual].

Ralph who had been a victim of ransomware wanted technical support that would make such an attack again unlikely:

Someone to come and check the antivirus. Check the normal file settings and stuff like that. Someone to trust. Even if, they don't have to come in. They can do an IT team viewer job thing. And just have a look and say, look, this is where it's failing. We suggest you do this. It takes about ten minutes. That's all you could have done. That would have helped. Ralph. [Ransomware, SME].

Aliya simply wanted to speak to someone with technical skills in the police who would understand her incident:

I think I would have liked to have been able to speak to an IT genius in this police force, or that that should land, my case should land on the desk of someone who really understood IT crime. Aliya. [Ransomware, SME].

Justin also wanted further technical support to reassure him that the website would now be resilient to future attacks:

I mean, well, you know, advice on...depending on how much they looked into it, obviously, I provided them all the information I provided to you about how the attacks took place. So, if they had come back with some feedback, so, you know, you've got an unsecured FTP server, you should really think about securing this, if you haven't already. Or something to say, that they've looked into how this had happened and steps we could take to prevent it. Hackers will do that stuff anyway, but it would be nice if they were providing that, sort of, feedback. Justin. [Hacking, SMO].

Henry wanted a website that would provide all the information necessary to do what is necessary:

I think that if they worked together to provide a website that you could just go to and say, right, this is what you need to do. And it's got a checklist for you of everything: the banks, Action Fraud, internet security. And also, of absolutely critical importance, information on how this functions, to give some sort of reassurance. You know, I can't emphasise enough for me, in particular, the need for reassurance and re-empowerment. And the sooner that could happen, the better. And so, with something like this, if there were a website that were available, that said well you've got to do all these things, of course you have, that goes without thinking. But then there are these resources, which will help you to feel better about what has happened. That, I think, will be absolutely superb. Because I don't think I'm alone in that feeling. And that, you know, that need to be reassured was as powerful as shutting everything down and doing all the responsible things. Henry. [Hacking, Individual].

As did Wayne:

Well, yes, I think had at my initial point of asking for help, had at that initial point somebody said, you know what, Wayne, we'll have a look at it, but in the meantime, please have a look at this website and these are the things you can do and these are things you can be getting on with, then that would have helped, rather than just the, we'll be in touch. Because even if you go on self-help websites, sometimes you think, you know, am I doing the right thing doing this, but if there was a UK government page, that would have helped me no end. Wayne. [Harassment, individual].

Sabrina wanted technical support that would immediately come and deal with an incident:

Technical knowledge, someone with technical knowledge. So, there's the immediate emergency of what happens, and we needed someone for that. Beyond that, there's a context that you're working in, there's an awareness that you are working in a digital context, and exactly as if you were in a university building, or if you were in a building that's on the high street, you wouldn't go out and leave your door unlocked when you leave the office that night, you wouldn't leave your data unprotected, that, we needed, and that we still don't have,

actually. I don't have a comprehensive knowledge, I have the knowledge I picked up through things that happened, but that's not the same as starting from the ground, and having someone explain to you, so you come out of something with, right, these are the things, these are my main priorities. I think we still need that, to be honest. Sabrina. [Hacking, SME].

Mary also wanted police with technical knowledge to work with to deal with the incident:

Someone who was an expert in cyber attacks who could give us meaningful avenues to pursue. Police resource to track down the perpetrators. Cooperation from platforms - Twitter/ 8 chan to cooperate with the police re passing on relevant details about the hackers. Mary. [Denial of service attack, SME].

Patricia thought police officers should be better trained in digital crime:

It's not great. I mean, if I could suggest anything, there needs to be better training around digital crime for sure. You know, harassment should not be...once it reaches a certain level, there needs to be a threshold, it should really be a TC because it's complicated. And there's very little...I mean, people like [inaudible 0:49:32] and Suzy Lamplugh Trust, they're overwhelmed. Patricia. [Multiple, individual].

What did I want the most? I didn't want it to obviously affect the business to the point where you can't take credit cards payments anymore, that's for sure, because that would have been the end which if it happens repeatedly they can do that, stop you from taking them. But, do you know, I don't know, I found the resources were very limited, there's hardly any help really apart from, unless you pay for a private body to do it for you. so there was very little assistance, which for an SME, you know, these people [inaudible 07:11] are incredibly expensive. Mathew. [Hacking, individual].

Offenders brought to justice

Several victims stated they wanted the perpetrators of the incident brought to justice:

I would love to have received they'd caught the perpetrator, that was the main purpose of my call. Terry. [Computer Virus, Individual].

Rachael reflected that although dealing with the incident and resolving it had been her immediate priority, on reflection she thought catching the perpetrators would have been good.

Yeah, I mean, getting rid of the problem, rather than catching the perpetrators, was my priority. But now, on reflection...at the time you can't help but think your political opponents are the ones who are responsible for it. I have no evidence of that obviously, and so on reflection, I would like people to be held accountable for that. Rachael. [Denial of Service Attack, Individual].

Joana also wanted to know that action was taking place to catch the perpetrators:

At the point of the incident, well I didn't really need...I didn't really...it wasn't the advice I wanted, it was the support I wanted, I wanted somebody to...I wanted to feel that this wasn't going to be getting away with it, you know. But there was no implication, it was, I think, this is the trouble with this global world, is that the more global it gets the more alone you feel, if

you see what I mean. 'Cause, oh, he's miles away oh we can't do anything about him, you know, it's just...and you're just little needle in the haystack, kind of thing, so, yeah, I didn't really need any advice 'cause I knew I'd, actually, been scammed and I'd been stupid, and I felt relieved. But what I did want to know is, I wanted to feel that this bloke sitting in his palace in Nigeria wasn't going to get away with it, but he's still doing it. Jonana. [Hacking, individual].

Just more support to track them down really, the people who'd done it. Mathew. [Hacking, individual].

Kate just wanted her ex-boyfriend to know he was breaking the law:

Yeah, I just wanted to protect myself from that happening again, from him, to let him know that that was breaking the law, and that is was a punishable kind of crime. Kate. [Hacking, individual].

Reassurance

Several victims mentioned reassurance as a need. These victims had been rendered feeling vulnerable as a consequence of the incident and desired some form of reassurance to help cope with it. Henry had almost lost a large sum of money an reassurance was very important to him:

In one word, reassurance. Reassurance, which was, I suppose, a form of re-empowering. I felt totally disempowered by that, because we've become so reliant on our phones and everything else and to have that invaded takes away your power. Henry. [Hacking, Individual].

Terry just wanted to be sure that criminals did not have information that could be used to target him as a result of the incident.

I think I just wanted reassurance that I hadn't...I knew I hadn't given them any information, but I just wanted assurance I wasn't going to be bugged again by them. Terry. [Computer Virus, Individual].

Lily also wanted reassurance:

For them to actually seem interested in investigating it, seeing who it was or where it came from and just reassurance that they wasn't going to take my money because I didn't know whether they had access to my online banking and stuff like that. In the 50 hours, I was going away for the weekend to London, and I was just worried that when I was away they would take all my money. So just like some reassurance. Lily. [Computer Virus, Individual].

10. Conclusion and Recommendations

This research has provided some important new data on victims of CMC. First it has shown that most victims regard CMC as an equivalent crime to traditional crimes like burglary, with some considering it more serious, with a small minority regarding it as a lesser crime. The research demonstrated victims experience many of the impacts that other crime victims experience, with some overlap with fraud.

There were also some victims who suffered severe impacts, as well as some noting very small impacts and regarding it as little more than disruption.

The research explored how victims fell victim and showed in some cases they were tricked by sophisticated social engineering, some exhibited poor security behaviours putting them at greater risk, but some also had very good behaviours but still fell victim. The research explored the changes in behaviour as a result of victimisation and it showed in general there were not major changes. The reasons victims did not report were examined and then the experiences of those that did. The response of the police and Action Fraud, where there was a response was also explored. The report ended by considering what the victims wanted.

The findings from this research lead the authors to make the following recommendations, which fall under the following categories: improving reporting, improving victim support and advice, increasing resources for tackling computer misuse.

Improving reporting

The experience of the researchers dealing with victims and trying to understand their interpretations of what happened illustrated the challenges of definition. This was highlighted further with data supplied by the NFIB, which showed there had been misclassification of victims, not just among web reporters. The research was conducted with data drawn before changes to the online reporting system and better quality checks were introduced. Many of these issues may therefore have already been addressed. However, it is essential that those reporting cybercrimes are properly classified for both measurement, investigation and response issues.

Recommendation 1. The new systems for reporting, classifying and ensuring the quality of decisions undertaken by Action Fraud and National Fraud Intelligence Bureau (NFIB) should be regularly monitored and evaluated to ensure the classification of CMC reports for both telephone and web reporting are being classified accurately [Directed at Action Fraud/NFIB].

The central challenge of the name Action Fraud is for many victims this does not sound like a body cybercrime should be reported to, particularly when it does not involve fraud. Another challenge to reporting CMC (and fraud) is the name Action Fraud and the association of the word 'Action' with investigation and response, rather than reporting. Some victims actually think it is a special fraud investigation squad, which implies there will be an investigation by Action Fraud. For these reasons the researchers think the name should be changed.

Recommendation 2. Action Fraud should be renamed the 'National Fraud and Cybercrime Reporting Centre' [Directed at Home Office, City of London Police].

This report identified a number of barriers to individuals reporting CMC offences. There are a number of recommendations below which aided with a focused communication strategy could enhance reporting:

Recommendation 3. Greater prominence should be made of CMC offences on the Action Fraud website [Directed at Action Fraud].

Recommendation 4. All police reporting websites should be reviewed to assess information provided on reporting CMC and where there are gaps advised to more clearly indicate how cybercrime can be reported with relevant links provided [Directed to Home Office and all police forces].

Recommendations 5. The NCSC should work with key bodies such as Action Fraud, Getsafeonline; relevant service providers, such as banks, social networking sites, email providers etc who receive cybercrime reports, to provide a common set of words and website links to be placed upon their website to encourage them to report as crime [Directed to NCSC, Action Fraud and relevant website providers].

There was also evidence of some staff who might receive or advise on reports did not grasp the legislation relating to CMC, particularly related to non-financial related crime such as harassment, voyeurism and domestic disputes where the research found examples of victims being wrongly advised their case was not a crime. The authors therefore suggest that all relevant police staff and Action Fraud staff should receive training in CMC offences and where such training already occurs, it should be regularly reviewed to ensure those experiencing it clearly understand what constitutes this type of crime, the seriousness of it and options for victims:

Recommendation 6. All police officers, police staff and Action Fraud staff dealing with victims who may report crimes should be better trained in what constitutes CMC offences, particularly in relation to non-financial related cases such as voyeurism, harassment and domestic disputes; and the options for dealing with them [Directed to Home Office, College of Policing, Action Fraud].

Improving victim support and advice

The findings noted limited changes in behaviour by some victims from the survey and interviews. There were examples of victims who were hacked not improving their password security and computer virus victims not engaging with anti-virus software. Some of the interview victims at the point of victimisation were clearly interested in cyber security, but were not offered appropriate tailored advice. This seemed to be a missed opportunity at the point of victimisation to enhance the resilience of the victim. The Economic Crime Victim Care Unit (ECVCU) pilot is an illustration of moves to more intensive support for this type of victim. This research has not evaluated the ECVCU and some of its activities would overlap with the following recommendation:

Recommendation 7. Tailored packages of advice/support (based on National Cyber Security Centre guidance/advice) relating to the specific type of incident should be supplied to the victim at the point of reporting and evaluation of this support should be undertaken regularly to improve it [Directed at Action Fraud and the NCSC].

Recommendation 8. Further research should be conducted to evaluate different approaches to targeting victims and the impact these have on behaviours and future victimisation [Directed at Home Office].

There was evidence of victims not receiving information on the progress of their case, which is contrary to the Victims Code. There was also considerable variation in the nature and extent of the responses victims received.

Recommendation 9. Action Fraud and the police should do more to ensure victims do receive timely information on what has occurred in relation to their case [Directed at the police and Action Fraud].

The Action Fraud website was the most recognised by victims, but the research team's views were that it was not necessarily the best at supplying information to victims on prevention, support etc of CMC related offences. Getsafeonline and the National Cyber Security Centre provided the best advice in the view of the research team, but were low down the recognition list of victims. Action Fraud could either develop new website or link in a more effective way to the better websites. It might also be

prudent to conduct some research with victims to determine the most effective websites for offering advice.

Recommendation 10. Action Fraud, with the most recognised website offering advice, should work with the National Cyber Security Centre to ensure consistent and technically accurate advice on preventing and dealing with cybercrime is provided to victims. This should also be built upon research to determine the most effective websites for interesting and changing the behaviour of victims [Directed at Home Office, Action Fraud, National Cyber Security Centre].

Increasing resources for tackling computer misuse

The findings for this research found many victims who did not receive a police investigation or any other form of police interest. Some victims did not want any police support, but many did. There were also cases where victims thought they had clear leads on who the offenders were (although in reality those leads may have been weak), but nothing occurred. It is clear that many victims who want police support do not receive it. There are clearly not enough resources of the police dedicated to CMC and many of the resources that do exist are built upon short-term funding, with no guarantee they will continue (HMICFRS, 2019). The authors believe more resources should be dedicated to this crime, how much, however, is clearly a political decision when there are so many demands on the police.

Recommendation 11. The police should dedicate greater resources towards tackling CMC [Directed at the Government, Home Office and the police].

It is clear that even with more resources the police could not fill the gap in the support that victims want. Technical support was one of the main needs identified by victims and many of the demands that fall under this would not necessarily be something the police could or should provide, particularly in relation to SMEs. There is a challenge, however, of where to go to secure technical advice and who to trust. There are other examples in physical security of official schemes to indicate compliance with standards and that the operator is a legitimate supplier such as the Security Industry Authority's Approved Contractor Scheme and the police service's Secured by Design initiative. The National Cyber Security Centre has a variety of certification programmes, but these do not currently cover providers of cyber security services at the front line of victims. A scheme that provides a kite mark of approval and list of suppliers that could be provided to individual and SME victims would aid them in securing appropriate professional support.

Recommendation 12. The Government should encourage a scheme to recognise suppliers who are accredited to appropriate standards to provide cyber security technical services to individuals and SMEs, similar to schemes such as Secured by Design and the SIA's Approved Contractors Scheme. Victims could then be provided with links to a website which includes a list of relevant suppliers who have met those standards [Directed at the Home Office and National Cyber Security Centre and the NPCC].

References

Button, M., Lewis, C. and Tapley, J. (2014) Not a Victimless Crime: The Impact of Fraud on Individual Victims and their Families. *Security Journal* 27(1) 36-54.

Etikan, I., Musa, S. A., and Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American journal of theoretical and applied statistics*, 5(1), 1-4.

Finnerty, K., Fullick, S., Motha, H., Navin, J., Button, M. and Wang, V. (2019) [Cyber Security Breaches Survey 2019](#). London: IPSOS Mori

Finnerty, K., Motha, H., Navin, J., White, J., Button, M. and Wang, V. (2018) [Cyber Security Breaches Survey 2018](#). London: IPSOS Mori

Furnell, S. (2002). Cybercrime: Vandalizing the information society (pp. 3-540). London: Addison-Wesley.

Klahr, R., Shah, J., Sheriffs, P., Rossington, T., Pestell, G., Button, M. and Wang, V. (2017) [Cyber Security Breaches Survey 2016](#). London: IPSOS Mori

Klahr, R., Amili, S., Shah, J., Button, M. and Wang, V. (2016) [Cyber Security Breaches Survey 2016](#). London: IPSOS Mori

HM Government (2019) Criminal Justice System Statistics publication: Outcomes by Offence 2008 to 2018: Pivot Table Analytical Tool for England and Wales. Retrieved from <https://www.gov.uk/government/statistics/criminal-justice-system-statistics-quarterly-december-2018>

HMICFRS (2019) Cyber: Keep the Light On. Retrieved from <https://www.justiceinspectors.gov.uk/hmicfrs/wp-content/uploads/cyber-keep-the-light-on-an-inspection-of-the-police-response-to-cyber-dependent-crime.pdf>

Leveson (2012). *An Inquiry Into The Culture, Practices and Ethics of The Press: Report*. Volumes 1 to 4. London: Stationery Office.

Levi, M., Doig, A., Gundur, R., Wall, D., Williams, M. (2015) The Implications of Economic Crime for Policing. Retrieved from <https://www.cityoflondon.gov.uk/business/economic-research-and-information/research-publications/Documents/Research-2015/Economic-Cybercrime-FullReport.pdf>

ONS (2019a) Crime in England and Wales: Appendix tables (Years ending December). Retrieved from <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables>

ONS (2019b) Crime in England and Wales: Additional tables on fraud and cybercrime (Years ending December). Retrieved from <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables>

ONS (2018a) User Guide to Crime Statistics for England and Wales. Retrieved from <file:///su2/U4/ButtonM/Downloads/Chrome%20Downloads/userguidetocrimestatistics.pdf>

ONS (2018b) Overview of fraud and computer misuse statistics for England and Wales. Retrieved from [file:///su2/U4/ButtonM/Downloads/Chrome%20Downloads/Overview%20of%20fraud%20and%20computer%20misuse%20statistics%20for%20England%20and%20Wales%20\(2\).pdf](file:///su2/U4/ButtonM/Downloads/Chrome%20Downloads/Overview%20of%20fraud%20and%20computer%20misuse%20statistics%20for%20England%20and%20Wales%20(2).pdf)

ONS (2017) Crime in England and Wales: Additional tables on fraud and cybercrime. Year ending March 2017 Table E7. Retrieved from <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables>

Spalek, B. (2006) *Crime Victims*. Basingstoke: Palgrave.

Appendices

Appendix 1. List of interview victims and type of offence

Name of Victim	Type	If SME/O Type	Computer Misuse Offence Category	Accounts/Devices Involved	Consequence
Gweneth	Ind		Computer Virus/Malware	PC	Disruption of PC use
Vanessa	Ind		Computer Virus/Malware	Laptop	Disruption of laptop use
Godfrey	Ind		Computer Virus/Malware	PC	Attempted fraud
Terry	Ind		Computer Virus/Malware	Mobile Phone	Attempted fraud
Oliver	Ind		Computer Virus/Malware	Laptop	Disruption of laptop use and attempted fraud
Jing	Ind		Computer Virus/Malware	Laptop	Disruption of laptop use
Lily	Ind		Computer Virus/Malware	Laptop	Disruption of laptop use
Steve	SME	Consultancy	Ransomware	PC	Ransom attempt
Nigel	SME	Farmer	Ransomware	PC	Ransom attempt
Aliya	SME	Online Marketing	Ransomware	Website	Ransom attempt
Ralph	SME	Arts Venue	Ransomware	Organisation's Computers	Ransom attempt
Arnold	SME	Engineering	Ransomware	Organisation's Computers	Ransom attempt
Kellie	SME	Care Services	Ransomware	Organisation's Computers	Ransom attempt
Mark	SME	IT Services	Ransomware	Servers	Ransom attempt
Harold	Ind		Hacking	Bank Account	Attempted fraud
Andrew	Ind		Hacking	eBay	Attempted fraud
Charlie	Ind		Hacking	Bank Account	Attempted fraud
James	Ind		Hacking	Twitter	Account takeover for marketing
Peter	Ind		Hacking	Email	Excessive spam mail
Hilda	Ind		Hacking	Bank Account	Attempted fraud

Ann	Ind		Hacking	eBay	Attempted fraud
Lizz	Ind		Hacking	Groupon	Attempted fraud
Alex	Ind		Hacking	Playstation and Twitter	Harassment
Claire	Ind		Hacking	Bank Account	Attempted fraud
Sophie	Ind		Hacking	Email	To prevent changing employment
Caroline	Ind		Hacking	Email et al	Attempted fraud
Catherine	Ind		Hacking	eBay and Facebook et al	Attempted fraud
Sarah	Ind		Hacking	Bank Account	Attempted fraud
Angeline	Ind		Hacking	Facebook	Attempted fraud (of her network)
Joanna	Ind		Hacking	Email Account	Attempted fraud
Kate	Ind		Hacking	Facebook account	Damage her reputation by ex-lover
Jerry	Ind		Hacking	Ali Express account	Attempted fraud
Benjamin	Ind		Hacking	Bank Account	Attempted fraud
Authur	SME	IT services	Hacking	Servers	Damage business
Leo	Ind		Hacking	Email and Cloud Account	To destroy evidence gathered for divorce proceedings
Jacki	Ind		Hacking	Facebook and Instagram	Account takeover for marketing
Bernard	Ind		Hacking	Bank Account	Attempted fraud
Michael	Ind		Hacking	Bank account	Attempted fraud
Cameron	Ind		Hacking (attempted)	Bank Account	Attempted fraud
Henry	Ind		Hacking/Computer Virus	Bank Account and PC	Attempted fraud
Sam	Ind		Hacking and Computer Virus/Malware/Ransom	Laptop	To access webcam to take personal pictures and

					conduct extortion
Husky	Ind		Hacking and Computer Virus/Malware	Laptop	To monitor evidence gathered for divorce proceedings
Paul	Ind		Hacking and Denial of Service Attack	eBay and Email Account	Attempted fraud
Natalie	SME	Bakery	Hacking	Bank Account	Attempted fraud
Kathy	SME	Plumbing and Heating Engineer	Hacking	Email	Attempted fraud
Mathew	SME	E-Commerce Retailer	Hacking	Website	To gather data on customers for fraud
Justin	SMO	Secondary School	Hacking	Website	Diversion of school website to porn site
Sabrina	SME	Online Publisher	Hacking/ DDoS	Website	Diversion of company website to terrorist group
Rachael	Ind		Denial of Service Attack	Gmail	Disruption of election campaign
Guy	SMO	Secondary School	Denial of Service Attack	Organisation's Cloud	Disruption of school websites/IT
Patricia	Ind		Multiple	Multiple	Harassment, to secure intelligence and damage reputation
Mary	SME	Popular website	Multiple	Organisation's computers, systems and website	To disrupt website
Wayne	Ind		Harassment (Hacking?)	Multiple websites	Harassment

Appendix 2. Demographics of survey and interview victims


Categories	Survey		Interviews	
	N	%	N	%
Gender				
Male	112	44.4%	25	48.1%
Female	140	55.6%	26	50%
Prefer not to say			1	1.9%
Age				
18-24	52	20.6%	2	3.8%
25-34	103	40.9%	11	21.2%
35-44	59	23.4%	11	21.2%
45-54	30	11.9%	9	17.3%
55-64	5	2.0%	10	19.2%
65-74	2	0.8%	5	9.6%
75+	1	0.4%	4	7.7%
Employment Status				
Employed/Self-employed	201	79.80%	37	71.2%
Looking after family/home	5	2.00%	0	0%
Student	14	5.60%	6	11.5%
Retired	4	1.60%	8	15.4%
Unemployed	20	7.90%	0	0%
LT Sick	5	2%	1	1.9%
Prefer not to say	3	1%	0	0%
Occupational Status				
Non-manual: professional	41	16.3%	30	57.7%
Non-manual: employers and managers	47	18.7%	7	13.5%
Non-manual: intermediate and junior non-manual	39	15.5%	3	5.8%
Manual: Skilled manual and own account non-professional	46	18.3%	2	3.8%
Manual: Semi-skilled manual and personal service	38	15.1%	1	1.9%
Manual: Unskilled	15	6.0%	0	0%
Other	16	6.3%	8	15.4%
Prefer not to say	10	4.0%	1	1.9%
Education				
Higher degree/postgraduate qualifications	31	12.3%	14	26.9%
First degree (including B. Ed.) Postgraduate diplomas/Certificates (inc. PGCE) Professional qualifications at degree level (e.g. chartered accountant/surveyor) NVQ/SVQ Level 4 or 5	57	22.6%	12	23.1%

Diplomas in higher education/other H.E. qualifications HNC/HND/BTEC Higher Teaching qualifications for schools/further education (below degree level) Nursing/other medical qualifications (below degree level) RSA Higher Diploma	43	17.1%	7	13.5%
A/AS levels/SCE Higher/Scottish Certificate 6th Year Studies NVQ/SVQ/GSVQ level 3/GNVQ Advanced ONC/OND/BTEC National City and Guilds Advanced Craft/Final level/ Part III/RSA Advanced Diploma	59	23.4%	8	15.4%
Trade Apprenticeships	2	0.8%	2	3.8%
O-Level/GCSE grades A-C/SCE Standard/Ordinary grades 1-3 CSE grade 1 NVQ/SVQ/GSVQ level 2/GNVQ intermediate BTEC/SCOTVEC first/General diploma City and Guilds Craft/Ordinary level/Part II/RSA Diploma	35	13.9%	7	13.5%
O-Level/GCSE grades D-G/SCE Standard/Ordinary below grade 3 CSE grades 2-5 NVQ/SVQ/GSVQ level 1/GNVQ foundation BTEC/SCOTVEC first/General Certificate City and Guilds part 1/RSA Stage I-III SCOTVEC modules/Junior certificate	18	7.1%	2	3.8%
Other qualifications (including overseas)	1	0.4%	0	0%
None of the above	6	2.4%	0	0%
Prefer not to say	0	0.0%	0	0%
Household situation				
Lived alone	51	20.2%	10	19.2%
Married/ live with partner	133	52.8%	27	51.9%
Lived with family	61	24.2%	10	19.2%
Lived with friends	4	1.6%	3	5.8%
Prefer not to say	3	1.2%	2	3.8%
Race				
White and Black Caribbean	1	0.4%	0	0%
English/Welsh/Scottish/Northern Irish/British	207	82.1%	48	92.3%
Irish	4	1.6%	0	0%
Gypsy or Irish Traveller	0	0.0%	0	0%
Any other white background	7	2.8%	2	3.8%
Any other Black / African / Caribbean background	1	0.4%	0	0%
Indian	5	2.0%	0	0%

White and Black African	3	1.2%	0	0%
White and Asian	6	2.4%	0	0%
Any other Mixed / Multiple ethnic background	0	0.0%	0	0%
Caribbean	4	1.6%	0	0%
Any other ethnic group	2	0.8%	0	0%
African	3	1.2%	0	0%
Arab	0	0.0%	1	1.9%
Pakistani	4	1.6%	0	0%
Bangladeshi	0	0.0%	0	0%
Chinese	2	0.8%	1	1.9%
Any other Asian background	2	0.8%	0	0%
Prefer not to say	1	0.4%	0	0%
Region				
North East	9	3.6%	2	3.8%
North West	30	11.9%	3	5.8%
Yorkshire and The Humber	17	6.7%	3	5.8%
East Midlands	19	7.5%	2	3.8%
West Midlands	29	11.5%	1	1.9%
East of England	17	6.7%	6	11.5%
London	43	17.1%	4	7.7%
South East	31	12.3%	22	42.3%
South West	22	8.7%	5	9.6%
Wales	13	5.2%	3	5.8%
Scotland	19	7.5%	1	1.9%
Northern Ireland	3	1.2%	0	0%
Prefer not to say	0	0%	0	0%

Appendix 3. Non-police reporting websites

<https://help.twitter.com/en/safety-and-security/twitter-account-hacked>

 **Help Center** [Help topics](#) [Guides](#) [Contact us](#)

Using Twitter ▾

Managing your account ▾

Safety and security ▲

- Security and hacked accounts
- Privacy
- Spam and fake accounts
- Sensitive content
- Abuse

Rules and policies ▾

Help with my hacked account

If you think you've been hacked and you're unable to log in with your username and password, please take the following two steps:

1. Request a password reset

Reset your password by requesting an email from the [password reset form](#). Try entering both your username and email address, and be sure to check for the reset email at the address associated with your Twitter account.


If you're able to log in after the password reset, please check if your [account has been compromised](#) and re-secure your account.

2. Contact Support if you still require assistance

If you still can't log in, contact us by submitting a [Support request](#). **Please choose "Hacked account" from the list of options.** Be sure to use the email address you associated with the hacked Twitter account; we'll then send additional information and instructions to that email address. Include both your username and the date you last had access to your account.

Learn more about what you can do if you've [lost access to the email account associated with your Twitter account](#).

<https://www.ebay.co.uk/help/account/protecting-account/get-help-hacked-account?id=4196#contactWay>

 **Search eBay Help...**

[What to do if your account has been hacked](#)

[Signs your account has been hacked](#)

If you think someone is trying to take over your account – or already has – we'll work with you to secure it. For your protection, we may place a temporary hold on your account.

Whenever there is suspicious activity related to your account, it's important to act quickly. If you think your account might have been compromised, first check if anyone with access to your account made changes to it, or used it to either buy or sell.

What to do if your account has been hacked

If your account has been taken over or compromised, the first step is to try and sign into your account.

If you can sign into your account

If you can still sign in, take the following steps:

1. [Change your password](#) immediately.
2. [Change your secret question](#).
3. [Verify your contact information and payment details](#). Check your contact information, your shipping addresses, and your payment information. If anything was changed by the person who took over your account, change it back.
4. Check your active bids and listings in [My eBay](#), to make sure they're yours. [Contact us](#) for help with removing unauthorised fraudulent bids or listings.

If there's been no fraudulent activity on your account, you don't need to contact us.

If you can't sign into your account

If you can't sign in to your account, [contact us](#) immediately.

Tip
If you believe your eBay account has been compromised, we recommend changing the password on your personal email account as well. Your email account password should be different from your eBay password.

Appendix 4. Action Fraud Reporting Website

The screenshot shows the top navigation bar with 'REPORT FRAUD CALL US 0300 123 2040' on the left, and 'CYMRAEG ENGLISH' and 'LOGIN' on the right. The main header features the 'Action Fraud' logo and a navigation menu with 'REPORTING', 'TYPES OF FRAUD', 'PREVENTION', 'NEWSROOM', and 'ABOUT US'. A search icon is also present. A dropdown menu is open under 'REPORTING', listing: 'Reporting fraud', 'Report a phishing attempt', 'Guide to reporting', 'Reporting in local language', 'Adroddiad yn gymraeg', and 'FAQs'. The main content area has a dark overlay with the text 'Start reporting' and 'Please select the option that best describes you:'. Below this is a form with the heading 'I am' and four options: 'A VICTIM', 'REPORTING FOR A VICTIM', 'A BUSINESS', and 'A WITNESS', each with a right-pointing arrow. To the right, there is a red banner that reads 'CYBER REPORTING FOR BUSINESSES' with a 'LEARN MORE' button below it. The background image shows hands typing on a laptop keyboard.

The screenshot shows the 'Action Fraud' logo and navigation menu at the top. Below the navigation is a breadcrumb trail: 'HOME > TYPES OF FRAUD > A-Z OF FRAUD'. The main heading is 'Computer hacking'. Below the heading is a social media share count of '420 SHARES' with icons for Facebook, Twitter, and LinkedIn. The article text begins with 'Computer hackers break into computers and computer networks.' followed by a paragraph: 'Computer hackers are then able to gain sensitive and personal information from the computer or computer network, which can be used to commit fraud. Fraud has been committed if money has been lost.' A second paragraph states: 'If your website is suffering from a Distributed Denial of Service (DDoS) attack - follow our advice here.' At the bottom, there is a 'See also:' section with links to 'Malware', 'Phishing', and 'Identity theft and fraud'.

Appendix 5. Police Reporting Websites

https://www.westyorkshire.police.uk/report-it

Home > Report it

Anti-social behaviour >	Criminal damage >
Domestic abuse >	Drink driver / drug driver >
Drug use / drug dealing >	Hate crime >
Lost and found property >	Nuisance bikes / quad bikes / off roaders >
Suspicious behaviour >	Terrorism >
Theft >	Report something else >

https://www.dorset.police.uk/do-it-online#report

Report something

Full crime report

Use this form to submit a full crime report, where you are the victim, or you are reporting it on behalf of the victim.

Report something else

Have something else to report to us? - Please use this form to report non crime related information to us. Please include as much information as possible to assist us with answering your enquiry.

Report a hate crime

Are you the victim of, or witness to, a hate crime or incident? Please let us know by using this form here.



Report lost or found property

Information on how to report lost or found property.



Report fraud or cyber-crime

Please use the National Fraud and Cyber Crime Reporting Centre to report fraud and cyber related incidents.



Report something anonymously

Please use CrimeStoppers if you'd like to report something anonymously rather than directly to Dorset Police...

Report radicalisation, terrorist and extremist behaviour

Advice on how to report concerns if you think that someone is at risk of radicalisation, is involved in terrorism, is promoting an extremist ideology, or if you are unsure or suspicious about somebody's activities or behaviour.

Partner Information Sharing and Request Form

Please note: this form is for use by agencies and professionals who work with vulnerable people. If you are a member of the public and you have concerns about a person being exploited please report it via the 101 Enquiry form or Crimestoppers.

GDPR form responses

The page lists the Force Command Centre (FCC) responses to 'What happens next' when you complete an online form on this website that goes to the FCC. This information has been provided as part of our response to the General Data Protection Regulation (GDPR).