'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]

'...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]
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of acronyms</td>
<td>2</td>
</tr>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Methods and profile of victims</td>
<td>3</td>
</tr>
<tr>
<td>Perception of computer misuse crime</td>
<td>4</td>
</tr>
<tr>
<td>Impact of computer misuse crime</td>
<td>4</td>
</tr>
<tr>
<td>The impact on victims in their own words</td>
<td>4</td>
</tr>
<tr>
<td>Financial</td>
<td>5</td>
</tr>
<tr>
<td>Disruption</td>
<td>5</td>
</tr>
<tr>
<td>Psychological impacts</td>
<td>5</td>
</tr>
<tr>
<td>Health impacts</td>
<td>5</td>
</tr>
<tr>
<td>Damage to reputation</td>
<td>5</td>
</tr>
<tr>
<td>Violation of the digital self</td>
<td>5</td>
</tr>
<tr>
<td>Loss of digital possessions</td>
<td>5</td>
</tr>
<tr>
<td>Falling victim</td>
<td>6</td>
</tr>
<tr>
<td>Security behaviours</td>
<td>6</td>
</tr>
<tr>
<td>Victims’ response to victimisation</td>
<td>6</td>
</tr>
<tr>
<td>Reporting computer misuse crime</td>
<td>7</td>
</tr>
<tr>
<td>Reasons for low reporting</td>
<td>7</td>
</tr>
<tr>
<td>Reporting experience</td>
<td>7</td>
</tr>
<tr>
<td>Advice and support received</td>
<td>8</td>
</tr>
<tr>
<td>Victims needs</td>
<td>8</td>
</tr>
<tr>
<td>Conclusions and recommendations</td>
<td>9</td>
</tr>
<tr>
<td>Improving reporting</td>
<td>9</td>
</tr>
<tr>
<td>Improving victim support and advice</td>
<td>10</td>
</tr>
<tr>
<td>Increasing resources for tackling computer misuse</td>
<td>11</td>
</tr>
</tbody>
</table>
# TABLE OF ACRONYMS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMC</td>
<td>Computer Misuse Crime</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>ECVCU</td>
<td>Economic Crime Victim Care Unit</td>
</tr>
<tr>
<td>CSEW</td>
<td>Crime Survey for England and Wales</td>
</tr>
<tr>
<td>HMICFRS</td>
<td>Her Majesty’s Inspectorate of Constabulary, Fire and Rescue Services</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communications Technology</td>
</tr>
<tr>
<td>NCSC</td>
<td>National Cyber Security Centre</td>
</tr>
<tr>
<td>NFIB</td>
<td>National Fraud Intelligence Bureau</td>
</tr>
<tr>
<td>NPCC</td>
<td>National Police Chiefs’ Council</td>
</tr>
<tr>
<td>ONS</td>
<td>Office for National Statistics</td>
</tr>
<tr>
<td>SIA</td>
<td>Security Industry Authority</td>
</tr>
<tr>
<td>SME/O</td>
<td>Small Medium Sized Enterprise/Organisation</td>
</tr>
<tr>
<td>2FA</td>
<td>Two Factor Authentication</td>
</tr>
</tbody>
</table>
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
- 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

‘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 in 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]

‘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]

‘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 net financial 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.
EXECUTIVE SUMMARY
VICTIMS OF COMPUTER MISUSE

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
- 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 was 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 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 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 a 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].
'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 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]