UNIVERSITY OF PORTSMOUTH

Victims of Computer Misuse Research

Professor Mark Button

Background

- Limited research on CMC and many questions
- Summer 2018 awarded grant by Home Office and HMIC to research victims of CMC
- Broad Aims were:
  - To examine the nature and impact of computer misuse related crime on victims; and
  - 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.

Research Undertaken

- Literature review
- Interviews with 7 stakeholders
- Survey undertaken by Qualtrics which secured 252 responses from victims of CMC
- Interviews with 52 victims of CMC (38 individual, 14 SME) + 1 SME written response
- Also reviewed websites where reports can be made, offering support etc

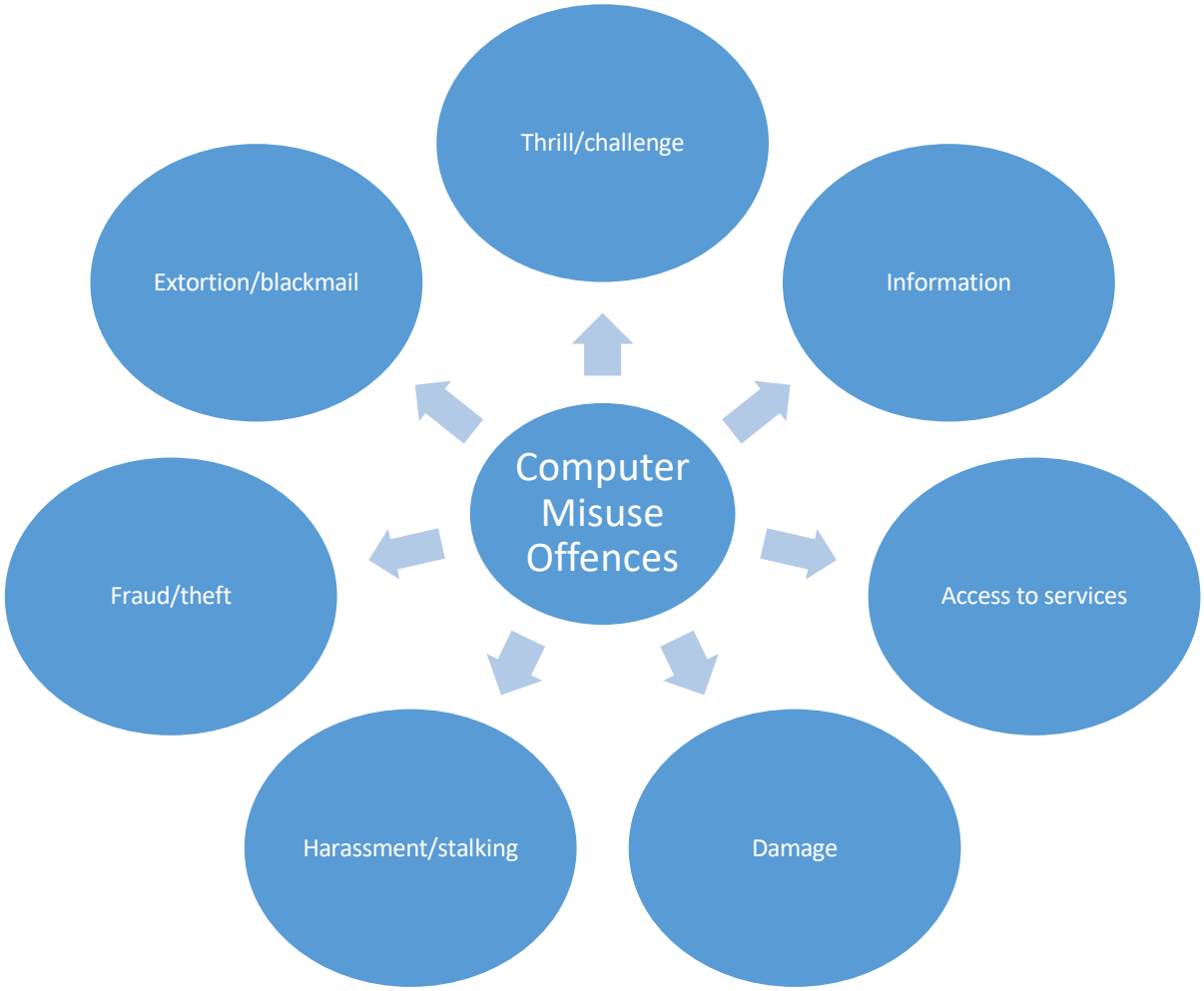
What is Computer Misuse Crime?

- Computer Misuse Act 1990
- *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.

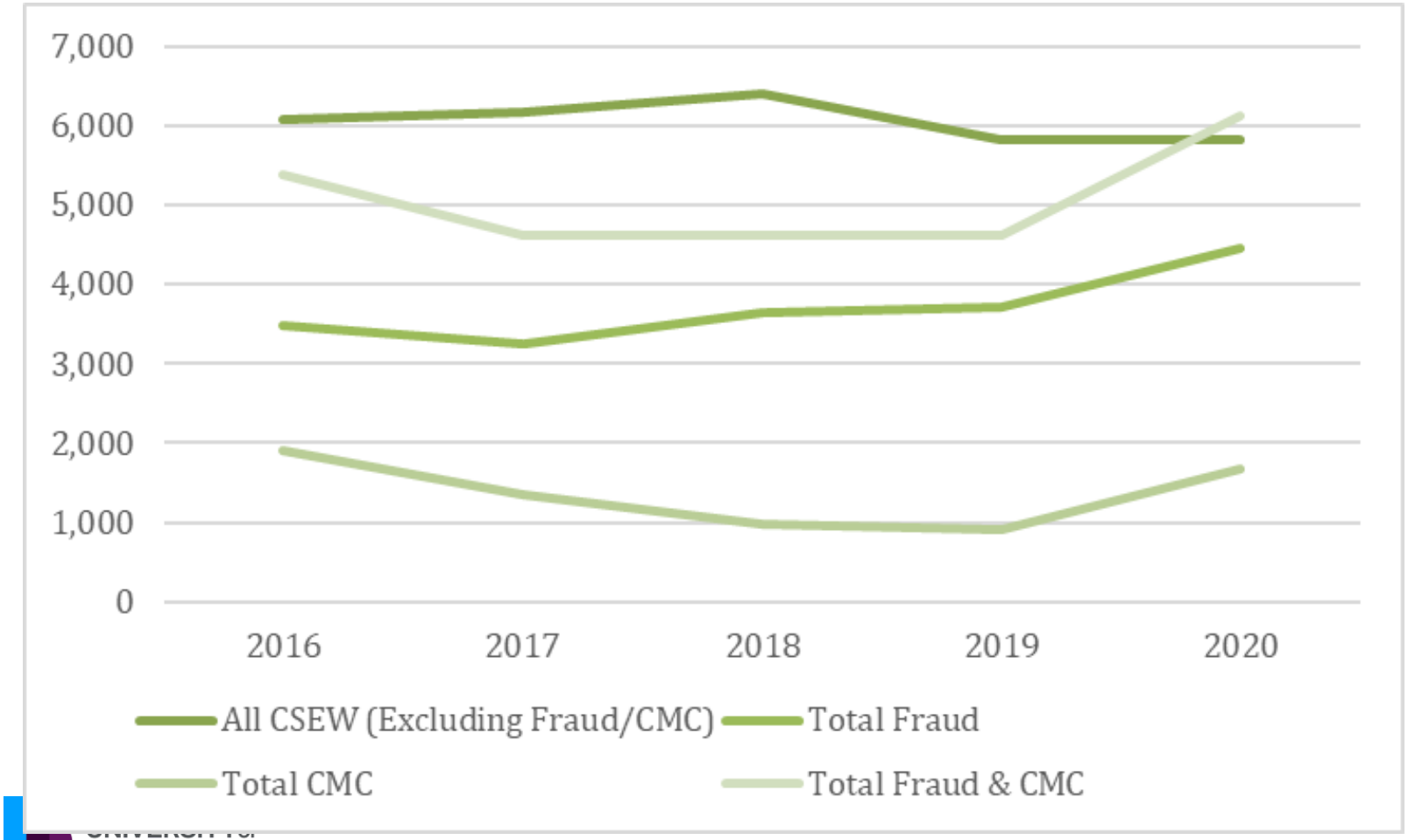
UNIVERSITY OF PORTSMOUTH

Computer Misuse Act 1990



UNIVERSITY OF PORTSMOUTH

Extent of CMC Crime: CSEW computer misuse offences in comparison to fraud and all other crimes (000s) year ending December 2016-2020



Recorded CMC by Action Fraud

	2014	2015	2016	2017	2018	2019	2020
Computer viruses/mal ware	5,535	4,108	5,208	7,954	5,215	5,536	7,192
Denial of service attack	160	249	579	332	254	136	116
Denial of service attack (extortion)	55	134	400	291	224	30	71
Hacking - server	452	532	610	724	841	298	332
Hacking - personal	2,375	2,532	3,358	3,652	3,973	2,996	4,915
Hacking - social media and email	5,637	5,355	4,484	7,792	8,936	11,101	14,004
Hacking - PBX/dial through	507	575	524	372	230	102	132
Hacking (extortion)	601	862	1,071	1,037	3,710	2,936	2,889
Total Computer Misuse	15,322	14,347	16,234	22,154	23,383	23,135	29,651

UNIVERSITY OF PORTSMOUTH

The Status and Impact of CMC: Victims' Perspectives

Types of victims in research

- **Interviews**
- 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.
- Adds up to 53 due to inclusion of ‘Mary’ who wasn’t interviewed, but supplied detailed written response.

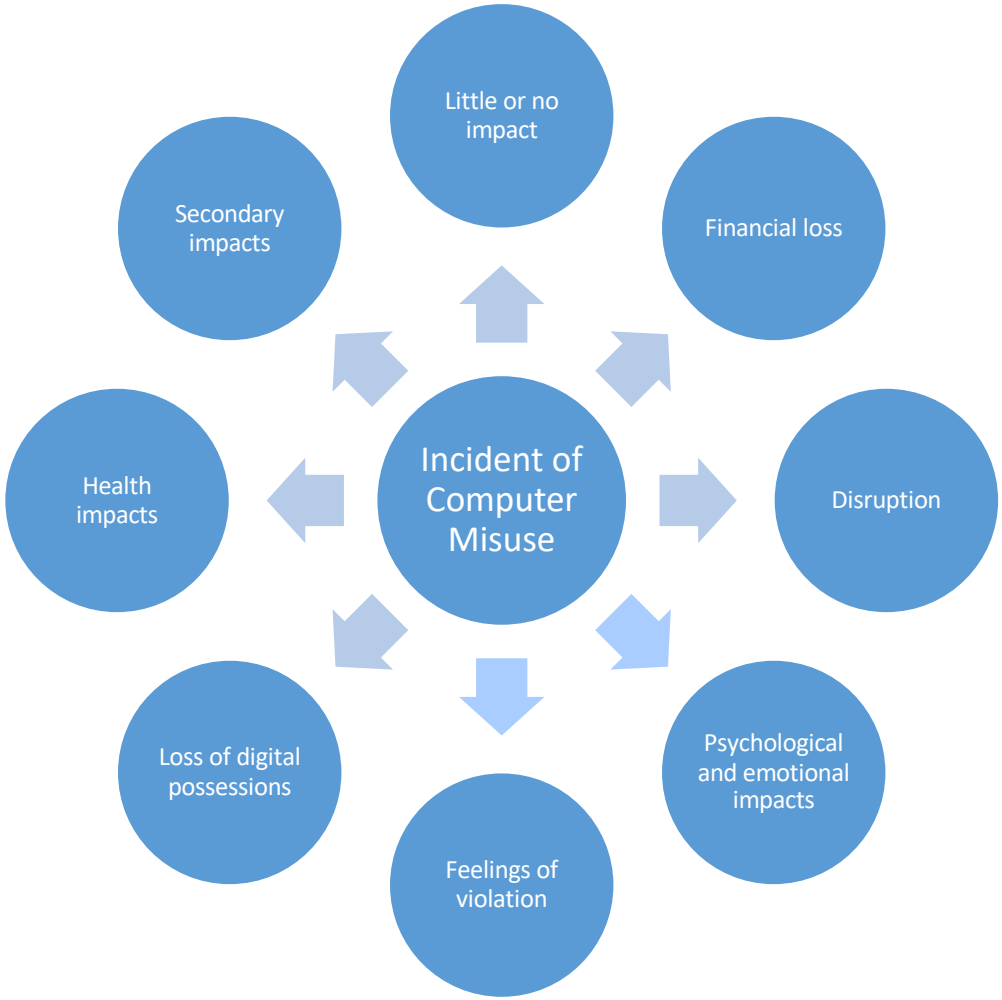
- **Survey**
- 49% - **hacking of an online account** to access personal information or services [email, social media, bank account etc.]
- 13% **hacking of a computer or other device** in your possession [laptop, smartphone, desktop computer etc.] to access personal information
- 29% - **a computer 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
- 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]

UNIVERSITY OF PORTSMOUTH

The Status of CMC: Survey Victims

	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

Impacts Found



UNIVERSITY OF PORTSMOUTH

Impact on CMC on Victims

- Full range of impacts associated with fraud and other volume crimes were found among victims
- There were some where nothing more than minor disruption with limited impact, but at other extreme there was very significant impact among some victims .
- **Financial and Disruption**
- The survey victims experienced financial losses ranging from £2 to £10,000, with a mean of £657 and median of £250
- Most experienced no loss and those that did much of loss was associated with consequences of the incident
  - 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. Claire [Hacking, Individual].

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

- Disruption was noted by ONS statistics as common impact
  - 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 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].

Psychological

	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%

Psychological ctd

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

Psychological ctd

- **Stress**
  - 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. 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].
- **Embarrassment and shame**
  - 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].

Violation of the digital self

- Electronic devices/online presence have become digital extension of physical self
- **Violation**
  - …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. [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].

Ctd

- 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].

- 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].

Loss of digital possessions

- **Extension of digital self**

- 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. Catherine. [Hacking, Individual].

- The other thing I was really annoyed about was I had to change my email address. Paul. [Hacking and Denial of Service Attack].

Health impacts

	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%

UNIVERSITY OF PORTSMOUTH

- **Exacerbating health conditions**
  - 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].
- **Mental health**
  - 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].

- **Suicide**
  - 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 India, really hard. Patricia. [Multiple, individual].

Secondary: changes in behaviour

	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%

UNIVERSITY OF PORTSMOUTH

- **Damage to Reputation**
  - 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].
  - 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].

- **Negative Changes in Behaviour**
- 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].
- Yes it has, yeah. And like I say I've got more paper forms now than I have on the computer, and we print out a lot of documents for the [animals], I just keep them down here and write them rather than go and…even I can't be bothered to do that now; I just write on the documents now. Go back to the old fashioned way. Nigel [Ransomware, SME].

UNIVERSITY OF PORTSMOUTH

Victims' Experience of Reporting, Support and Investigations

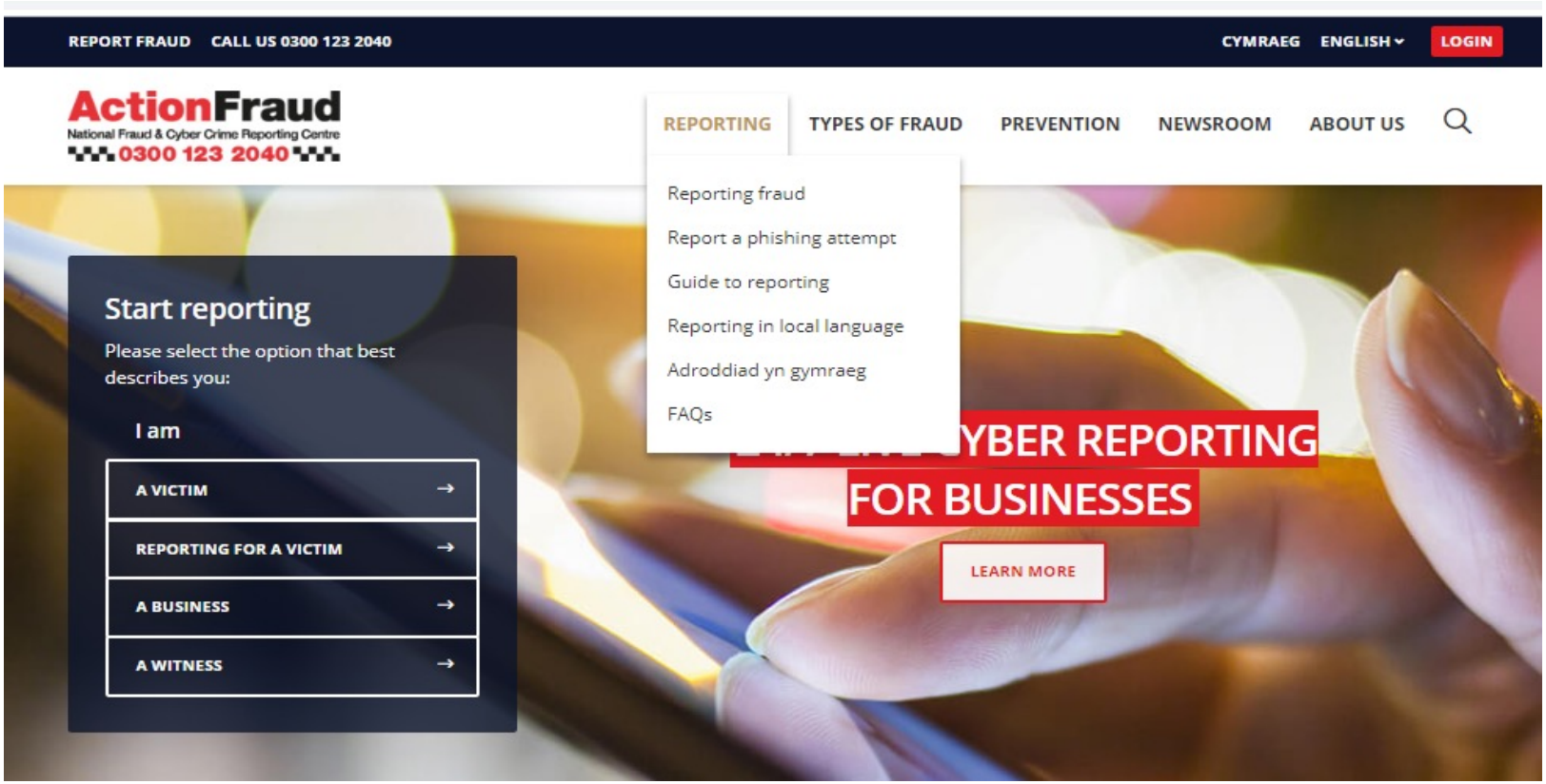
Reasons for Low Reporting to Police/Action Fraud

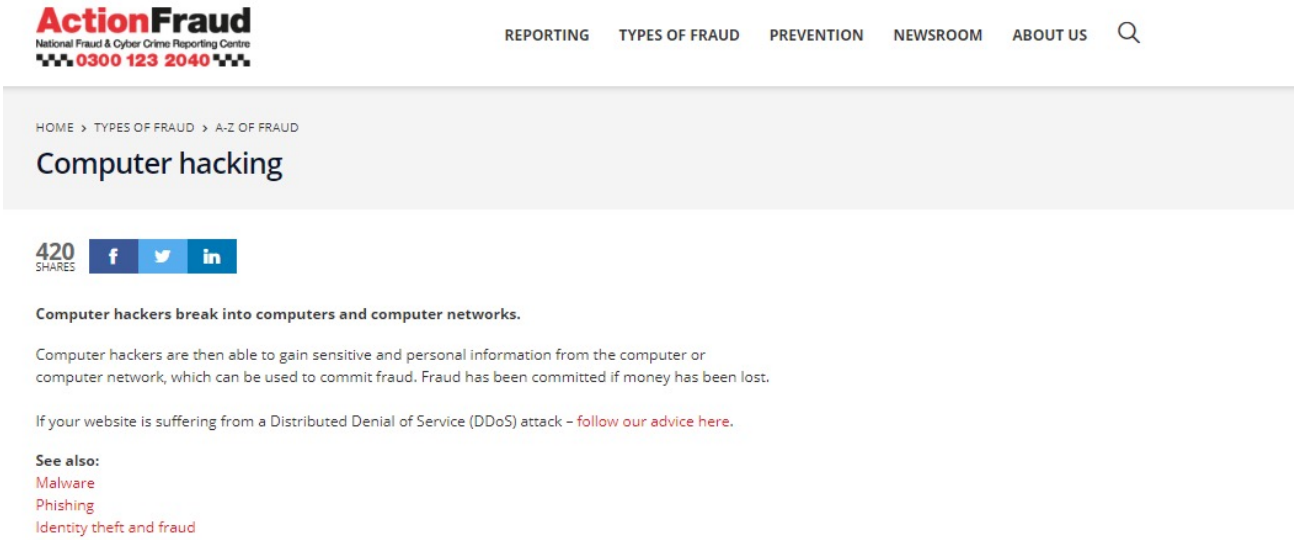
- Status of CMC
- No financial loss
- Assumption non-police/Action Fraud initial reporting body would pass on
- Reputation and experience of Action Fraud
- The police are unlikely to do anything because they are too busy
- Wrongly advised it was not a crime
  - And he [the police officer] said, you are married, so if you leave it [the laptop] on the table, he's got access.. Husky [Hacking, individual].
  - 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].
- Never heard of Action Fraud

UNIVERSITY OF PORTSMOUTH

Ctd

- Embarrassment and fear of the consequences of reporting
- Other websites where CMC is reported
- Action Fraud website
- Police reporting websites





UNIVERSITY OF PORTSMOUTH

Police response

- **Visit or contact from the police to take a statement or provide support**
  - 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].
- Leads to pursue
  - 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].

- Police investigation – very few received
  - 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].

A few weeks later

  - …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].

Successful Investigation

- 1 Victim Case Resulted in Police Caution
  - 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].
- 3 Victims Experienced NCA Successful Case – Very Positive
  - 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].
  - 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].

UNIVERSITY OF PORTSMOUTH

UNIVERSITY OF PORTSMOUTH

Falling Victim and the Needs of Victims

Falling Victim

- The Weak Point
  - **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].

Ctd

- **Victims with poor security habits**
- **Passwords**
  - 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'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].

Ctd

- Anti-Virus
  - 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].
  - 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].

Ctd

- Risky Behaviours
  - So, it was probably from any of the number of sites that I used to stream, like TV things on. Vanessa. [Computer Virus, 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].
- Lack of engagement with security standards for SMEs
  - 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].

UNIVERSITY OF PORTSMOUTH

Victims with good security habits

- 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].
- 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].

UK Government

BEATING CRIME PLAN

BEATING CRIME PLAN

Fewer victims, peaceful neighbourhoods, safe country

July 2021

We will restrict the opportunities that fraudsters seek to exploit. We are working with the tech, financial, telecoms and accountancy sectors and will seek to agree sector charters with commitments to strengthen firms' defences. The forthcoming Online Safety Bill will require tech companies to tackle fraud, giving firms the responsibility of protecting their users from fraud. We will examine the case for additional regulation to tackle harms such as fraud disseminated via paid-for advertising online.

We will make it harder for fraudsters to target the UK. Since its launch last year, the National Cyber Security Centre has shut down over 50,000 scams and taken down almost 100,000 websites.

We will improve our understanding of how fraudsters are operating. We will replace Action Fraud with an improved national fraud and cybercrime reporting system and increase intelligence capabilities in the NCA and the national security community to identify the most harmful criminals and organised criminal gangs.

We will take fraudsters off the streets and increase arrests and prosecutions. We will increase law enforcement investigative capacity in the City of London Police, as national lead force for fraud, and in Regional Organised Crime Units across England and Wales. We will also establish a new fraud investigative function in the NCA to target the most complex and serious fraudsters, meeting a manifesto commitment to create a new national cybercrime force focused on fraud.

We will provide better support for the victims of fraud. We want to expand the National Economic Crime Victim Care Unit and make public communications more coherent and coordinated.

- We will publish a new National Cyber Security Strategy later this year. The Strategy will drive significant improvements in the UK's response to cybercrime. It will strengthen the Law Enforcement response and drive greater collaboration with the National Cyber Security Centre and the National Cyber Force.
- We will publish a new strategy for tackling hate crime this autumn, setting out our commitment to stamping out these abhorrent crimes including their online elements, which cause greater harms to victims and associated neighbourhoods.
- We will set out further plans this summer for driving down online racist abuse as part of our response to the Commission on Race and Ethnic Disparities report.
- We will amend legislation to extend the use of Football Banning Orders so online abusers can be banned from stadiums, in the same way that violent thugs are barred from grounds. The change will be brought forward as soon as practical.

Joint Fraud Taskforce

Information about the Joint Fraud Taskforce (JFT), including membership, meeting minutes and the sector-based charters to combat fraud.

From: Home Office
Published 17 October 2017
Last updated 29 October 2021 — See all updates

Contents

The Joint Fraud Taskforce (JFT) is a partnership between the private sector, government and law enforcement to tackle fraud collectively and to focus on issues that have been considered too difficult for a single organisation to manage alone.

It will drive public-private action on fraud through the oversight of implementation of the Fraud Action Plan and assure progress against voluntary sector agreements with industry, the fraud sector charters.

The JFT relaunched on 21 October 2021, following a review of its role, structure and objectives.

UNIVERSITY OF PORTSMOUTH

5. Questions

Reports

- https://pure.port.ac.uk/ws/portalfiles/portal/20818541/Victims_of_Computer_Misuse_Executive_Summary.pdf
- https://pure.port.ac.uk/ws/portalfiles/portal/20818559/Victims_of_Computer_Misuse_Main_Findings.pdf

UNIVERSITY OF PORTSMOUTH