The Cyber Helpline

Supporting victims of cybercrime

The UK criminal justice system is failing victims of cybercrime

The Funnel of Justice: Understanding Reporting Gaps, Judicial Outcomes and Taxonomic Concerns in Cybercrime and Online Harm Victimisation

Written by Charlotte Hooper

October 2024

Abstract

The Home Office states that over 40% of crimes in England and Wales are fraud, the vast majority of which are online crimes. To get a full picture of online crime, we need to look at all forms of cyber-enabled and cyber-dependent crimes. This report finds that 58.4% of crimes in England and Wales utilise technology. Yet, when compared to the rates across all crime types, victims of cybercrime and online harm are over 40% less likely to report the crime and seven times less likely to see the perpetrator of the crime charged or summonsed.

Introduction

Cybercrime and online harms are rapidly evolving, impacting millions of individuals annually in England and Wales alone. Despite their increasing frequency and complexity, the gaps in reporting, investigating, and achieving judicial outcomes for these crimes result in a lack of justice, closure, and a sense of safety for victims. This report combines The Cyber Helpline's data with data from across the UK to explore these pitfalls from the point of victimisation through to successful prosecution.

Victims of cybercrime experience violent impacts in numerous areas of their lives, from their mental health to their physical safety to their financial status; the ability to report and achieve justice for the crime is a critical step in their recovery. However, significant gaps in understanding cybercrime and online harms leave victims wanting and needing more. This report aims to explore these gaps, focusing on the stages of the justice system where attrition is particularly significant and seeking to identify the factors that contribute to this. These stages include reporting, investigation and prosecution.

This report aims to provide a clear understanding of the dynamics of response to cybercrime and online harms by discussing these parts of the funnel. It highlights the need for improved reporting mechanisms, refined taxonomies, and an overhaul of the investigative framework for these crimes. Crucially, victims of cybercrime need pathways to justice that are clear, inclusive, and provide fairer outcomes for all.

The real impact of cybercrime and online harms

Whilst this report centres on the analysis of systemic gaps, it is essential to recognise the impact that cybercrime and online harms have on the individuals experiencing them, to truly acknowledge the urgency of addressing these issues.

Therefore, this section centres on the voices of those who have lived through these experiences, to remind us that the pain inflicted through digital crimes is real. Much of the data on the impact of cybercrime and online harms focuses on the funds lost, but the impact reaches far beyond this; the voices of victims provide a reminder of why justice is important and why rethinking how we address and respond to cybercrime is an urgent matter. Service users of The Cyber Helpline have provided these quotes; each has given their consent for their quote to be used.

> "The cost of recovery has been financially crippling and repetitive. I ended up in rent arrears unable to pay my rent, bills and had to flee to another city… It has cost me £8000 in recovery and damages but I still haven't recovered…"
>
> Victim of identity theft on the financial impact

> "I have lost weight, eaten by stress. I am unable to sleep. And I am up-down emotionally. I feel so low and afraid. I am a ghost of my former self."
>
> Victim of a loan scam on the impact on their mental health

> “I don't feel safe. My face. My body. My tattoo is exposed...I feel physically sick, I'm in fear of my life, my job, my family or friends ever seeing it.
> If he wanted to scare me, he definitely has. I am afraid of him of what he will do and the lengths he would go just to hurt me. “
>
> Victim of intimate image abuse on their impact on their safety

> “I'm frightened to plug my TV in. I'm frightened to get broadband. I have got rid of every electronic device.I feel like I'm still being watched and listened to “
>
> Victim of stalking on the impact on their online confidence

> “I blamed over and over my partner.. because my stalker would steer my attention towards little things that made him look guilty, he will never see me the way he did before I repeatedly accused him.”
>
> Victim of stalking on the impact on others

> “I am spending all my spare time after work dealing with screenshotting evidence, trying to reset devices and reset passwords, it is draining me of energy. I am lying awake at late hours of night worrying about if my account is being looked at while I am asleep. “
>
> Victim of hacked email accounts on the impact on their day-to-day-life

Methodology, Limitations of Available Data and Justification of Categorisation and Assumptions

This report combines data from existing literature, datasets, and resources available in the public domain with The Cyber Helpline's data from users of its service in the UK.

For secondary data, data from the Home Office or Office for National Statistics has been prioritised; however, where this is not available, other data sources have been sought.

The Cyber Helpline provides support to victims of over 30 different types of cybercrime; however, published law enforcement data is limited and the current crime codes are much more basic than The Cyber Helpline's attack taxonomy. Due to the limits of the publicly available data, this report will focus on three key areas. These three categories are:

- crimes that fall under the Computer Misuse Act (CMA) and fraud;
- stalking and harassment and;
- Intimate image abuse.

The Crown Prosecution Service[1] provides a list of offences covered by the CMA:

- Unauthorised access to computer material;

- Unauthorised access with intent to commit or facilitate the commission of further offences;
- Unauthorised Acts with intent to impair, or with recklessness as to impairing the operation of a computer;
- Unauthorised acts causing, or creating risk of, serious damage;
- Making, supplying or obtaining articles for use in offence under Section 1, 3 or 3ZA.

Therefore, as Table 1 shows, it is believed that crimes falling under the CMA cover a plethora of the crime categories that The Cyber Helpline supports.

For Home Office and police forces data, there is often overlap between different crimes and harms; by using more recent data, the overlap will be accounted for due to changes that mean conduct crimes are recorded as the sole offence if deemed the most serious [2]. This means that this is likely to be the first year we can get an accurate representation of the funnel of justice for these crimes with minimal overlaps present.

For CMA and Fraud cases in particular, victims of these crimes may be individuals or organisations. This report is focused on individuals impacted by cybercrime. However, the data available in the public domain does not always distinguish between the two. As a result, for the purposes of this report, it is assumed that the experience of both victims and organisations in the funnel of justice is broadly similar. However, priority has been given to data that provides insight into individuals as victims where it is available.

In 2021, the Suzy Lamplugh Trust, a charity which runs the National Stalking Helpline, reported that 100% of their cases involved a cyber element. Yet, several police forces have reported much lower figures and there are significant variations between forces in recording the extent to which stalking crimes had an online element even in the same year, for example, 79.12% [3] and 13.31% [4]. Sussex Police[4] also noted in its response to a Freedom of Information request for the information, "Please note this data relies on officers manually ticking the Cyber flag therefore this data may not be fully accurate". The 'cyber flag' was implemented by the Home Office to 'flag' any cases reported by police forces as cyber-related. However, it does not appear to be fully utilised across many forms of cybercrime [5,6]. This may be due to officers not being aware of the 'cyber flag' [7], but it also relies on victims being aware of there being a cyber element and, if they are, disclosing it. The Cyber Helpline considered making FOI requests for the number of cases and outcomes, which included a a cyber-element for each crime type relevant to this report. However, due to the variations in utilisation of the 'cyber flag', this was deemed unfeasible as it would not present an accurate picture of the nature of cybercrime. Instead, for CMA and fraud, and intimate image abuse, we have assumed that 100% of cases are either cyber-enabled or cyber-dependent and 90% for stalking and harassment.

CMA and Fraud data from the Home Office was easily findable using the Home Office's [8] crime outcomes as they are categorised together. However, data from crimes falling under stalking, harassment, and intimate image abuse(for example, hate offences) were more challenging to find and to identify as cyber-enabled. As mentioned previously, based on previous third-party

research, we can assume that cyberstalking and harassment cases almost always have an element of cyber. For intimate image abuse, with various legal changes making this a relatively new type of crime, published data was limited. Therefore, FOI requests were submitted to gather this data.

Table 1 shows how The Cyber Helpline's taxonomy has been split between the categories. In some cases, there may be overlap between categories. In this case, the category in which it is thought to be most likely to be included in the published data has been chosen.

CMA and Fraud	**Intimate Image Abuse**	**Stalking and Harassment**	**Not included (not thought to be covered by official statistics on CMA and fraud or stalking and harassment)**
Encrypting Ransomware	Intimate Image Abuse/Revenge Porn	Online Harassment	Online Grooming
Screen-locking Ransomware		Cyberstalking	Lost device
Content for Ransom		Outing	Accidental information Share
Webcam Blackmail		Fake Profiles	Online Reporting Issue
Malicious Software		Fraping	Service Provider Breach
Hacked Email Account		Inappropriate Content	
Hacked Social Media Account		Bugs, Cameras and Trackers	
Hacked Online Bank Account			
Hacked Virtual Currency Account			
Hacked Online Gaming Account			
Hacked Online Shopping Account			

Hacked Home WiFi Network			
SIM Swapping			
Catfishing			
Phishing			
Vishing			
Smishing			
Virtual Currency Scams			
Card Fraud			
Identity Theft			
Online Auction Fraud			
Covid-19 Scams			
Cyber scams			
Recruitment Scams			
Loan scams			
Investment scams			

Table 1 - Table of categorisations of The Cyber Helpline's taxonomy

Data from The Cyber Helpline is drawn from entries by service users into The Cyber Helpline's chatbot, where demographics, issue description, and whether or not they had reported to the police were self-disclosed. The case was then diagnosed by The Cyber Helpline's chatbot and given a valid attack type from the typology, utilising machine learning technology built in-house and subsequently verified by an internal threat intelligence team.

The methodology for gathering this data is discussed throughout the report to provide context for calculations.

Quotes throughout the report have been obtained from service users of The Cyber Helpline who have completed an Impact Survey - this survey is optional for service users when accessing help through The Cyber Helpline. Participants have provided consent for their statements to be used for marketing and research purposes.

Reporting

The Crime Survey of England and Wales 2006/07 showed that just 1% of adult internet users who experienced hacking or unauthorised access in the previous 12 months had reported this

to the police. In comparison, 81% reported a burglary[9]. In 2013, McGuire and Dowling put this down to a number of reasons.

Why are cyber crimes underreported?

- *Perceptions that the police will not/cannot do anything about online crimes;*
- *not knowing where to report;*
- *reporting to other bodies such as banks or internet service providers;*
- *perceptions that cyber crimes are not 'real' crimes like, for example, vehicle theft or burglary;*
- *victims not realising or perceiving themselves as victims, for example, because a bank has refunded lost money, or being unaware that malware has infected their computer and stolen their personal details; and*
- *some victims simply being too embarrassed to come forward, for example, regarding common scams.*

-McGuire and Dowling (2013)

Whilst McGuire and Dowling's research is more than 10 years old, our work confirms that their findings remain valid. They also acknowledged the problems in measuring cybercrime and differing definitions; whilst they referred to this within research, this is also relevant in the policing landscape, leading to a lack of clarity on what cybercrime is, making responses, policy and perception of legislation vary by jurisdiction and individual[10] .

The Cyber Helpline has found that reports for cybercrime are still low. In the 1st quarter of 2024 (1st January 2024 - 31st April 2024), only 35.9% of The Cyber Helpline's service users (n=1,765) had disclosed to The Cyber Helplines chatbot that they had reported the issue to the police or a reporting body, such as Action Fraud.

We estimate that the number of people who report is still much lower than this for several reasons; the reasons listed by McGuire and Dowling[9] for victims not reporting the crime to the police continue to be relevant to some service users that may benefit from support from The Cyber Helpline. For example, victims of cybercrime may not always realise that they are victims - and, as such, are not in a position to seek support[11] .

> "They had all my personal information including bank and home address. When I was being threatened he said he would make sure I couldn't report it to the police. I have still not told anyone in case they come for me or hurt my children."
>
> Victim of fraud

McGuire and Dowling[9] anticipated an improvement in the quality and quantity of recording and identification of cybercrime through Action Fraud, for the cases that they cover, and the

implementation of the voluntary cyber 'flag' by the Home Office. However, Action Fraud has caused additional barriers to reporting; in March 2024, it took an average of over 10 minutes for a call to be picked up, and over 35% of calls were abandoned without speaking to an advisor[12] .

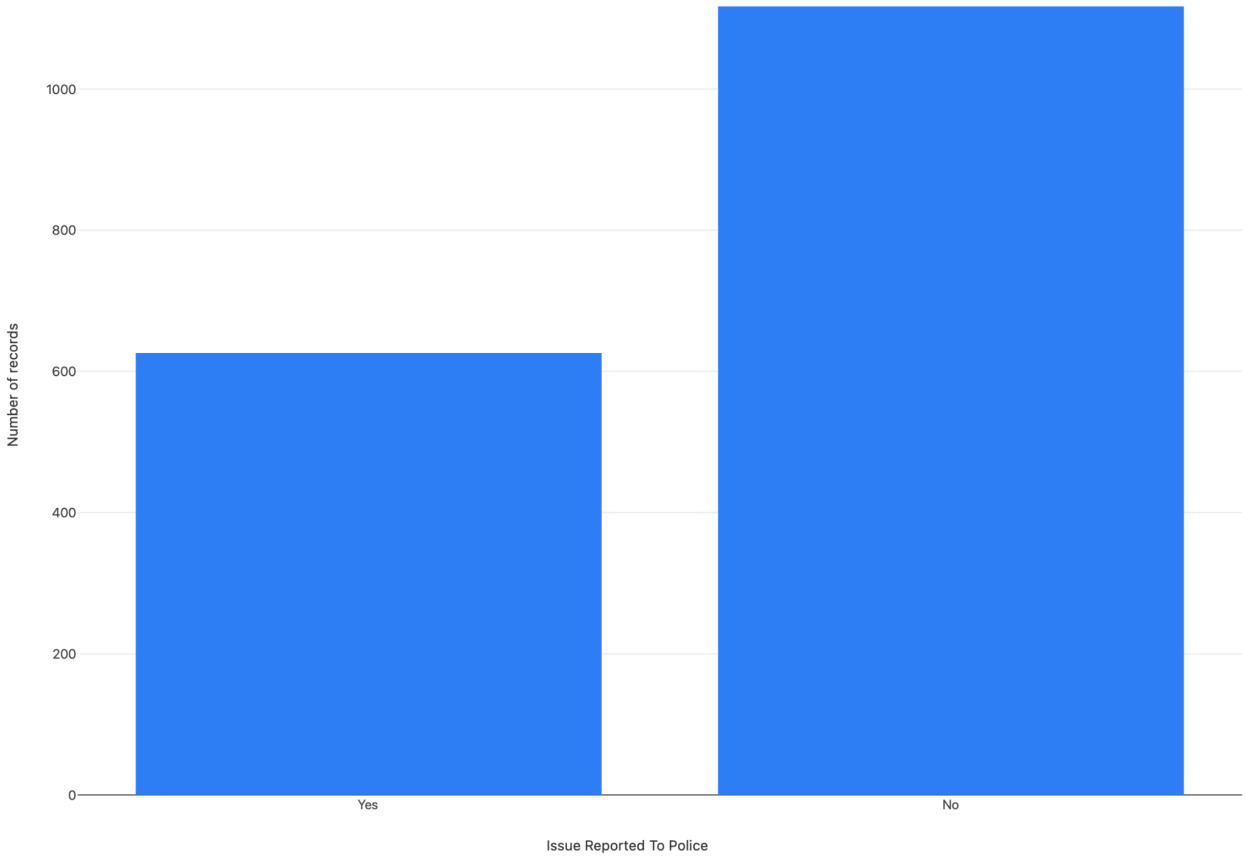

Figure 1 - Graph of the self-reported number of issues reported to the police from The Cyber Helpline's service users between the 1st January 2024 and 30th April 2024.

CMA and Fraud

Of service users who reported experiencing crimes under the CMA or fraud (n=1,143), only 33.2% said that they had reported the issue to the police.

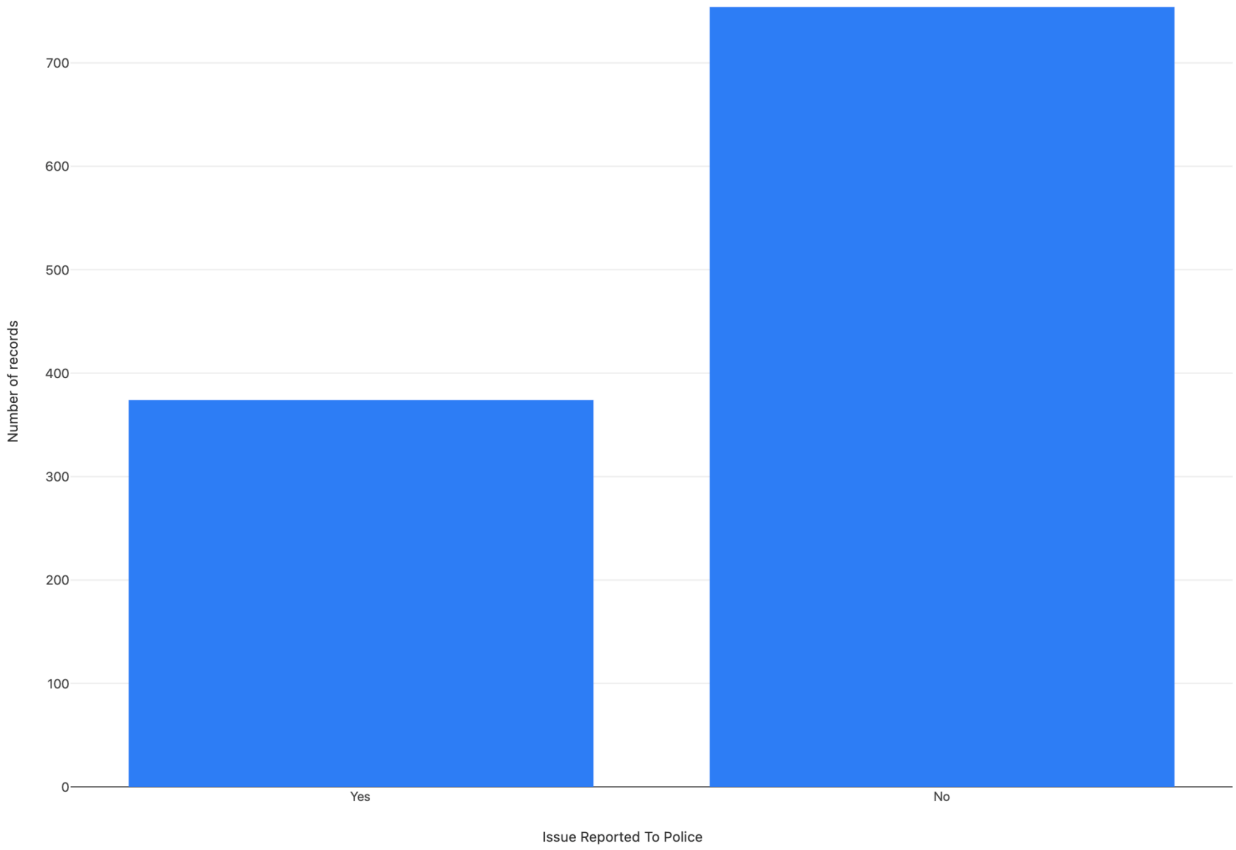

Figure 2 - Graph of the self-reported number of issues reported to the police from The Cyber Helpline's service users reporting experiencing crimes under the CMA or fraud between the 1st January 2024 and 30th April 2024.

Stalking and Harassment

The Suzy Lamplugh Trust[13] noted that 100% of their cases involved an element of cyber, yet there are significant variations between forces utilising the cyber flag when recording stalking and harassment offences. This appears to have caused an under-representation of online offending in cases within the criminal justice system and Home Office statistics. The number of stalking and harassment cases flagged as online crimes recorded by police in England and Wales, excluding Devon and Cornwall, made up only 23% of the total stalking and harassment cases in the year ending June 2023[14] . Given the varied use of the cyber flag, we have assumed that 100% of cases involve an element of stalking in line with the Suzy Lamplugh Trusts findings.

Complicating matters further, Home Office data does not readily distinguish stalking from harassment and the available data was limited. Nor did our literature review identify any data that could provide an estimate of the number of harassment cases involving an element of cyber.

For this research we have assumed that 90% of harassment and 100% of stalking cases contain an element of cyber. Nevertheless, it is still likely that these figures will be an underestimate of the true nature of stalking and harassment due to the covert nature of cyber-enabled and dependent stalking in many cases and the lack of realisation of the criminality and impact in harassment cases.

The Office for National Statistics[2] states that 663,526 stalking and harassment offences were reported to the police in the year ending December 2023, marking a 6% decrease in reports on the previous year. This is the first year since 2012 that stalking and harassment cases have decreased. However, this is likely due to the previously mentioned changes in recording.

42.31% of victims of stalking and harassment in the UK who have sought help from The Cyber Helpline (n=520), had reported to law enforcement.

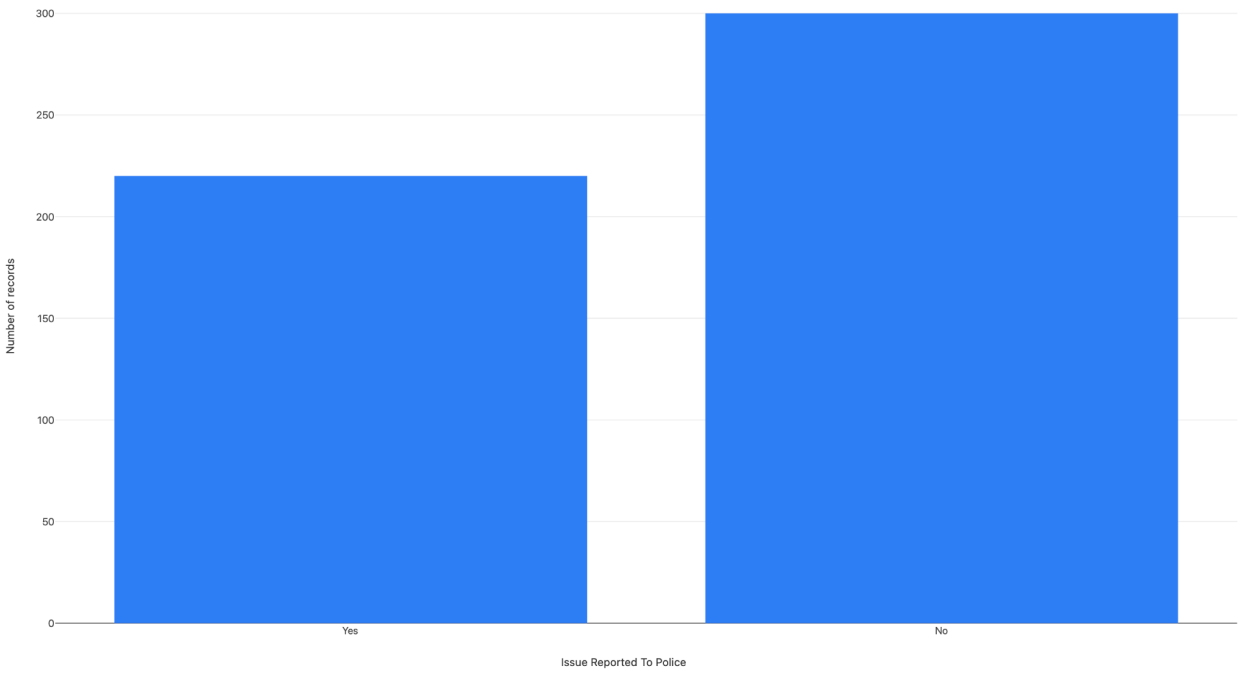

Figure 3 - Graph of the self-reported number of issues reported to the police from The Cyber Helpline's service users reporting experiencing stalking or harassment between the 1st January 2024 and 30th April 2024.

Intimate Image Abuse

Of those reporting intimate image abuse (n=46) to The Cyber Helpline, only 32.61% had reported to the police, despite the implementation of Section 66B of the Sexual Offences Act 2003, which implemented revised laws regarding intimate image abuse available for a majority of the period examined.

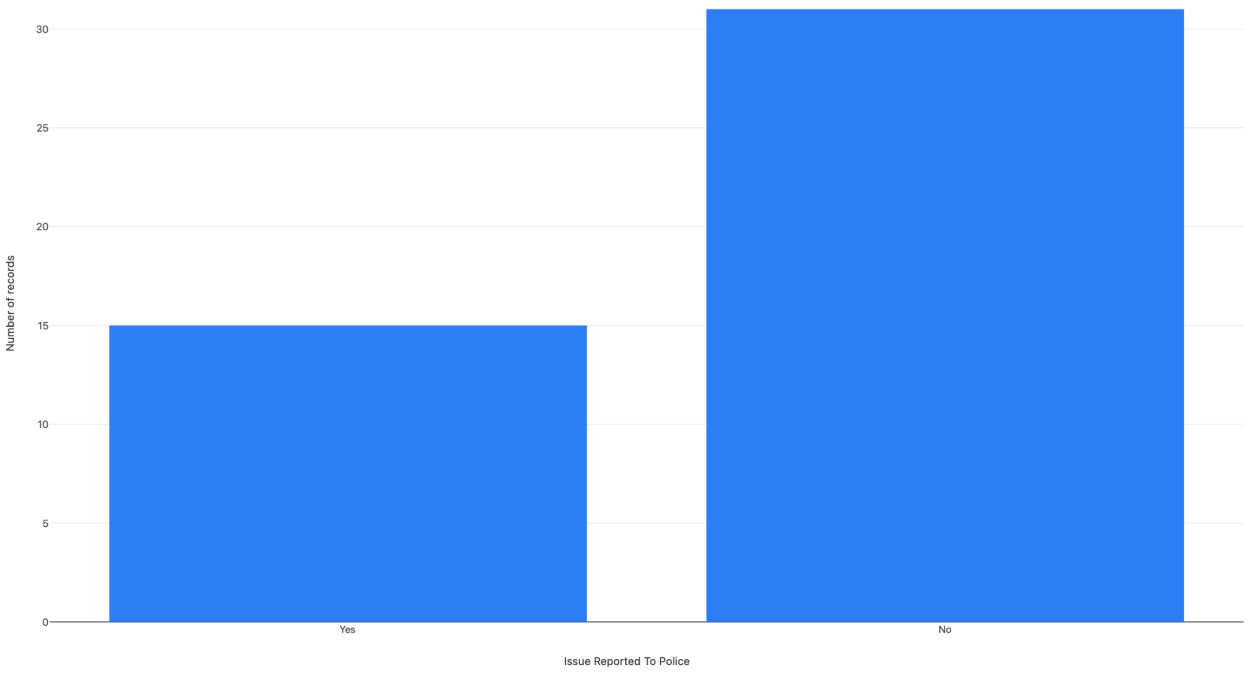

Figure 4 - Graph of the self-reported number of issues reported to the police from The Cyber Helpline's service users reporting experiencing intimate image abuse between the 1st January 2024 and 30th April 2024.

Investigation and Prosecution

CMA and Fraud

Of Computer Misuse Act (CMA) and Fraud offences recorded by Action Fraud, Cifas and UK Finance (n=1,151,192) (the latter two do not report CMA offences), discounting Devon and Cornwall Police as the data is not available, only 1.87% (n=21,546) were referred to local police forces between March 2022 and March 2023, a decrease of 32% on the previous year[8] .

According to the Home Office[8] , of CMA and Fraud offences recorded and disseminated to local police forces by Action Fraud, Cifas and UK Finance (n=1,151,192) (the latter two do not report CMA offences), discounting Devon and Cornwall Police as the data is not available, only 48,257 had an outcome recorded, a 17% decrease from the previous year. The outcomes, as reported by the Home Office[8] , can be seen in Table 2 and are tagged with the following six key themes:

[1] Formal action taken against perpetrator (red)

[2] Assumed/unclear if action taken against perpetrator (orange) - the reasons for these being unclear are that:

- For 'action undertaken by another body/agency' we are unaware of the outcome.
- For 'Taken into consideration' cases, we do not know the outcome of the charge it was taken into consideration for.

- For the remaining three outcomes, it's unclear whether actions were taken against the perpetrator, as these could be interpreted as actions taken to support or educate the victim, for example.

[3] No further action - Evidential or attribution difficulties (blue)

[4] No further action - not in the public interest (green)

[5] No further action - prosecution prevented (purple)

Outcome	Number of cases	% Change between previous year
Action undertaken by another body/agency [2]	1,524	-5%
Caution - adults [1]	454	+1%
Caution - youths [1]	21	0%
Charged/Summonsed [1]	3,962	-20%
Community resolution [1]	461	-12%
Diversionary, educational or intervention activity resulting from the crime report has been undertaken and it is not in the public interest to take any further action [2]	321	41%
Evidential difficulties (suspect identified; victim supports actions) [3]	10,479	-15%
Evidential difficulties (victim does not support action)[3]	8,422	-13%
Evidential difficulties: suspect identified, victim does not support further action [3]	5,612	-8%
Evidential difficulties: suspect not identified, victim does not support further action [3]	2,759	-23%
Further investigation to	1,442	-42%

Outcome	Number of cases	% Change between previous year
support formal action not in the public interest [4]		
Investigation complete - no suspect identified [3]	21,063	-18%
Not in public interest (CPS) [4]	44	-37%
Not in public interest [4] (Police)	203	-40%
Offender died [5]	35	-87%
Out of court (informal)[2]	461	-12%
Out-of-court (Formal)[2]	476	0%
Penalty notices for disorder [1]	1	-100%
Prosecution prevented - suspect underage[5]	6	100%
Prosecution prevented - Suspect too ill[5]	34	3%
Prosecution prevented - victim/key witness dead/too ill[5]	178	35%
Prosecution prevented or not in the public interest[5][1]	521	-42%
Prosecution time limit expired[5]	21	-48%
Taken into consideration [2]	157	+44%

Table 2 - number of cases and percentage change from the previous year of outcomes of reported crimes falling under CMA and Fraud in the year ending March 2023

Overall, this appears to show that, of the 1,151,192 cases recorded:

- 0.3% (n=2939) are unclear whether action was taken against the perpetrator;
- 0.4% (n=4899) appear to have action taken against the perpetrator;

[1] As this outcome includes prevention of prosecution and not in the public interest, it has been added to category 5 as this is listed first.

- 4.2% (n=48,335) appear to have had no further action taken due to evidential or attribution difficulties;
- 0.1% (n=1689) appear to have had no further action taken due to further action not being in the public interest;
- Less than 0.1% (n=795) had prosecution prevented;
- The remaining cases with no outcome available add up to 95% (n=1,092,355). This is not explained in the report but is assumed to be cases that have not been disseminated and, as such, have had no further action taken by the agencies they have been reported to.

The numbers and percentages provided by the Home Office do not appear to sum. For example, the records add up to 58,137, whereas the total number of outcomes reported by the Home Office[8] in the same table is 48,257. It is unclear why this is the case, but it is likely due to human error and/or unknown outcomes at the time of data submission. Furthermore, it is worth noting that the Home Office[8] states that these are Experimental Statistics and exclude Devon and Cornwall police due to availability issues.

In all, it appears that 99.4 to 99.7% of CMA and fraud cases have no further action taken after being reported.

Stalking and Harassment

There is a less comprehensive view of the outcomes of the 663,526 reported cases of stalking and harassment[2] , of which we estimate 90% (597,173) included an element of cyber. The Home Office[8] states that in the year ending March 2023 a majority (66.1%) of cases were closed due to evidential difficulties, 43.6% were closed due to victims no longer supporting police action. Charge rates were 3.4%, an increase of 0.3% from the previous year[8] .

However, The Suzy Lamplugh Trust[15] found through their research that only 1.4% of reported stalking incidents resulted in a conviction; we anticipate this number would be similar for harassment cases.

For the purpose of this report, we estimate that 100% of stalking and 90% harassment cases involve an element of cyber, and so for calculations, we will continue to use this figure. The significant limitations in the data which we have described above make it impossible to establish any differences in outcomes between stalking and harassment cases (online or not).

Intimate Image Abuse

Data on the number of intimate image abuse cases reported in the UK was limited. The Cyber Helpline submitted FOI requests to the 43 local police forces in England and Wales. Responses were received from all forces, apart from Essex Police and Dyfed Powys Police - as a result, figures for these areas are excluded from this report. However, it is unlikely that this has skewed the results significantly.

The Freedom of Information request asked for the number of "revenge porn" crimes recorded in the calendar year 2023 (to December) and the number of crimes resulting in four key outcome types:

- outcome type 1 (charged/summonsed);
- outcome type 14 (Evidential difficulties: suspect not identified; victim does not support further action);
- outcome type 15 (Evidential difficulties: suspect identified; victim supports action);
- outcome type 16 (Evidential difficulties: suspect identified; the victim does not support further action).

Four outcome types were requested in the FOI to maximise the chances of a response.

The responses to our FOI request showed that 8277 cases were recorded across the 41 local police forces. Not all of these had been assigned outcome types at the time of the FOI submission, and not all of these fell under the four outcome types chosen.

Outcome	% of cases
Charged/Summonsed	3.71%
Suspect not identified, the victim does not support further action	8.46%
Evidential difficulties: suspect identified; victim supports action	23.33%
Suspect identified, victim does not support further action	36.09%

Table 3 - outcomes from intimate image abuse cases in the calendar year 2023 (Essex Police and Dyfed-Powys Police cases are not included)

Victimisation

CMA and Fraud

The Home Office[8] stated that 1,151,192 incidents were reported to CMA and fraud reporting bodies in 2023 throughout England and Wales and yet only 33.2% of The Cyber Helpline's service users in the UK stated that they had reported the crime to the police. With this in mind, it is realistic to estimate that there are around 3,500,000 victims of CMA crimes and fraud in England and Wales every year, two-thirds of which are missing from official statistics due to not reporting.

Stalking and Harassment

The Office for National Statistics[2] states that 663,526 incidents were reported to the police in the year ending December 2023, whilst 46.36% of The Cyber Helpline's service users experiencing these crimes in the UK disclosed that they had reported the crime. This suggests that there are around 1,431,288 victims of stalking and harassment in England and Wales every year, with just under 1 million missing from official statistics due to not reporting.

Intimate Image Abuse

By looking at the 8277 reported incidents of intimate image abuse in England and Wales and The Cyber Helpline's findings that 32.61% of their service users report the crime, we can estimate that there are 25,381 victims of intimate image abuse in England and Wales every year, with over two-thirds being unreported.

What is the real picture of cybercrime?

CMA and Fraud

Stage	# of Victims progressing through stage	% of victims progressing through stage
Victimisation	3,467,446 (The Cyber Helpline)	100%
Reporting	1,151,192[8]	33.2%
Investigation/Dissemination	21,546[8]	0.62%
Charged/summonsed	4,899[8]	0.14%

Table 4 - estimated number of victims progressing through each stage of the funnel of justice per year in CMA and Fraud cases in England and Wales

Stalking and Harassment

Stage	# of Victims progressing through stage	% of victims progressing through stage
Victimisation	1,412,055 (The Cyber Helpline)	100%
Reporting	597,173[2]	42.31%
Charged/summonsed	20,304	1.44%

Conviction	8,360[15]	0.59%

Table 5 - estimated number of victims progressing through each stage of the funnel of justice per year in stalking and harassment cases in England and Wales

Intimate Image Abuse

Stage	# of Victims progressing through stage	% of victims progressing through stage
Victimisation	25,381 (The Cyber Helpline)	100%
Reporting	8,277 (FOI request)	32.61%
Charged/Summonsed	307 (FOI request)	3.71%

Table 6 - estimated number of victims progressing through each stage of the funnel of justice per year in intimate image abuse cases in England and Wales

Overall

Stage	# of Victims progressing through stage	% of Victims progressing through stage
Victimisation	4,904,882	100%
Reporting	1,754,476	35.77%
Charged/Summonsed	25,510	0.52%

Table 7 - estimated number of victims progressing through each stage of the funnel of justice in cybercrime and online harm cases per year, excluding online grooming and other categories in column 3 of Table 1 in England and Wales

All crime types

In order to compare the funnel of justice for cybercrime to other crime types, table 7 shows a calculation of the funnel of justice over all crime types. The calculations and sources of data are as follows:

- Charged/Summonsed - Home Office[8] shows that 312,167 crimes in England and Wales resulted in a charge/summons in the year ending March 2023. As this data does not contain fraud offences, these have been added to this figure from Table 4.
- Reporting - Home Office[8] shows that a total of 5,480,135 offences were recorded in the year ending March 2023, although 438,991 of these were awaiting an outcome. As the number of cases pending an outcome was not available for previous calculations, the total number of reported offences will be used to make a fair comparison. As this data does not contain fraud offences, these have been added from Table 4.

- Victimisation - Findings from the Crime Survey of England and Wales[2] led to the estimation of 8.4 million victims of crime in England and Wales in the year ending December 2023.

Stage	# of Victims progressing through stage	% of Victims progressing through stage
Victimisation	8,400,000[2]	100%
Reporting	6,631,327 (Home Office, 2023)	78.94%
Charged/Summonsed	317,066[8]	3.77%

Table 8 - estimated number of victims progressing through each stage of the funnel of justice in all crime types in England and Wales.

Comparing crime and cybercrime

Comparing all crime types to cases of cybercrime and online harm, we can see that victims experiencing cybercrime and online harm make up 58.4% of all victims of crime.

Despite this, only 35.77-35.9% of victims of cybercrime and online harms (listed in Table 1) have reported the crime to the police, compared to 78.94% for all crimes. This report shows over a 40% difference between those who report cybercrime and those who report crimes in general.

Furthermore, there is a clear difference between charged/summonsed outcomes within cybercrime and general crime, with crimes overall seven times more likely to be charged or summonsed than crimes involving an element of cyber, as listed in Table 1.

Why is this the current state of cybercrime?

Funding and Resource

The National Fraud Strategy[16] acknowledges that less than 1% of police resources are dedicated to cybercrime despite it accounting for over 40% of crimes[17] . Work is needed to improve reporting and increase understanding of the true nature of cybercrime and online harms to ensure that funding and resources are proportionate. However, this is not the only issue. Bowles et al.[18] note that the estimations of costs of cybercrime often exclude other factors, such as intimidation by the offender, the impact on individuals is not fully considered and understood, and crimes, such as technology-facilitated domestic abuse often have an effect further than any financial loss that has been experienced. For this reason, Bõhme[19] argues that the impact of cybercrime must be considered from not only an economic perspective but a psychological perspective - something that is currently rarely done within UK policing or wider society.

Barriers to Reporting

With only a small number of victims of cybercrime and online harm reporting the crime to law enforcement in the UK, when compared to other crimes, it is essential to understand why this is the case. McGuire and Gowling[9] provided their thoughts on this, including not knowing where to report, shame and not thinking anything could be done. However, Sikra et al.[20] expand on this, feeling that there is a cyber-responsibilisation agenda used by the UK government which takes a preventative approach to cybercrime by attempting to equip UK citizens with advice and then putting the onus upon them to follow it. Their theory is that, because of this agenda, victims feel too embarrassed to report, and this makes reporting a traumatising event.

Ways of reporting cybercrime in England and Wales also appear to be confusing. Sikra et al.[20] and Curtis and Oxburgh[5] note this, stating that Action Fraud is the only system available to accept reports on fraud. This becomes confusing for victims who are told that all crimes are reportable to the police.

> “I have reported everything to action fraud and the police but sometimes the reports are closed within minutes. The police often pass the issues onto safer neighbourhood team or the local resolution team. I have to make multiple complaints to even obtain a crime reference number. By the time this is obtained the evidence may have been edited, deleted or stolen.”
>
> Victim of Cyberstalking

Institutional Challenges

Correia[21] states "The criminal justice itself is based on a retributive model and not in a restorative one, focusing in the offender and in punishment." The criminal justice system is limited in the support it can provide an individual; its focus is on the offender, and there is no standardised approach to the support that a victim of cybercrime is offered after experiencing a cybercrime. This is especially pertinent when government-commissioned reports have found that officers fail to provide adequate support and show a lack of understanding of the risks facing victims, thus, a lack of empathy [7,22]. Boyce and Wood[23] argue that this needs change, and that compensation should extend beyond financial to psychological therapy that focuses on victimhood trauma.

> “Police think I'm crazy and treat me like I'm on drugs, and I was told by the police I shouldn't own a phone”
>
> Victim of a Hacked Social Media Account

Sikra et al.[20] note that researchers have various recommendations on how cybercrime should be policed. They split these researchers into two categories: those who feel cybercrime should be policed using the same approach as traditional policing and those who feel that this is inefficient given the current state of cybercrime training in England and Wales.

It is not only policing that shapes the funnel of justice, the demands of insurers increase the likelihood of reporting. For some crimes, such as burglaries, victims may need to report the incident to the police to be able to make an insurance claim, creating a formal incentive for victims to notify police and contributing to higher reporting rates. The lack of an equivalent requirement for cybercrime may reduce reporting rates. However, it is likely that this is due to change with more insurers releasing Personal Cyber Insurance which covers a limited range of cybercrimes.

Research indicates that those who belong to marginalised groups, such as people of colour and transgender people, are more likely to experience cybercrime and online harm[24,25] . There is a perceived lack of inclusivity in data collection and reporting systems. For example, the Action Fraud dashboard[26] shows only options for "male", "female", and "unknown" when recording victim gender. The absence of other gender identities reflects a limited understanding of victim demographics and may discourage individuals who do not identify within the given framework when they are only presented with these options when reporting.

Investigative Challenges

There are numerous challenges in understanding and investigating cybercrime and online harm within policing in England and Wales, including the lack of clear guidance for officers. Hadlington et al.[27] found that police officers felt ill-equipped to deal with cybercrime, confused about definitions and felt they needed training to help them keep up to date; this is a common theme throughout research and is backed by Curtis and Oxburgh's[5] study, finding that 61% of police officers in England and Wales felt they had insufficient training and experience to handle cybercrime cases.

The training that does exist does not appear to be effective, with one study finding that officers thought training around cybercrime was unstructured and not formalised or that it was not relevant to their role[28] . Meanwhile, Bossler et al.[29] surveyed officers across England and Wales and found that they felt they would be more prepared to support those impacted by online fraud when there were clear policies and procedures to follow.

Curtis and Oxburgh[5] found there to be a shortage of specialist tools and forensics capabilities to investigate and prosecute cybercrimes, with backlogs for forensics often taking months and even years due to a lack of resources; during this time, victims are left without their device(s), and this can lead to cases being dropped by victims who's devices may also be their connection to others, a source of income or even a safety net.

Taxonomic and Jurisdictional Challenges

The law is not necessarily equipped for policing cybercrime and online harm in the modern day. Whilst the Online Safety Act[30] was a big step towards changes in the criminalisation of online harms, there is still a long way to go for crimes occurring online as a whole.

At the time of access (11th May 2024 at 5:38 pm), Action Fraud's public dashboard showed that the most common crime code reported by individuals was NFIB 90, 'none of the above', evidence that the current taxonomy for cybercrime does not appear to be relevant for the crimes experienced by individuals.

But this may not be the first problem to solve; the definition of 'cybercrime' as a whole is still up for debate, as are the classification systems that accompany varying definitions; for this reason, Phillips et al.[10] proposed a new typology of cybercrime and online harms which encompasses varying attack types into a variety of different categories including interpersonal violence, sexual violence, using advanced technology and using false information. However, it neglects that cybercrime and online harms could fall into multiple of these categories; for example, cyberstalking, which falls under their sexual violence category and is separated from harassment despite their similarities in action and placement in UK legislation, could utilise illegal access, identity theft, harassment, incitement of violence, image-based abuse, hate speech, deepfakes and misinformation all in one, leading to one crime being categorised under seven of their eleven categories. Taxonomies and frameworks of cybercrime and online harm need to adapt to reflect overlaps and discrepancies in perpetrators' modus operandi, motivation and offline behaviours.

Jurisdictional issues, such as determining where a cybercrime occurred and which law enforcement agency is responsible, also create significant barriers to effective investigation and prosecution[15] .

International Comparison - Australia

ReportCyber, an Australian national policing initiative previously known as the Australian Cybercrime Online Reporting Network (ACORN) operates similarly to ActionFraud It is an online reporting system operating with no investigative capacity and instead forwards cases to relevant authorities. However, a key difference is that they accept cases of online harms, as well as financial crimes. Those reporting through the system are able to obtain updates on their case through the reporting portal.

Despite some improvements in the system, Voce and Morgan[31] found that most cybercrime in Australia still appears to go unreported and many victims reporting to ReportCyber stated they had not been contacted following their report (ranging from 18.8-25.9% depending on the type of crime) or told that their case would not be investigated (23.6-24.4%). As a result of the report, between 2.5-6.1% of victims were told that an arrest, charge or prosecution had taken place. As a comparison, the overall rate in the UK is believed to be 1.53%.

Limitations

Conducting this research relied on restricted data sets that had variations in crime codes and taxonomies. This has been addressed by combining taxonomies into three core areas, as seen in Figure 1. However, this lack of standardisation, whilst highlighting an issue in current definitions and taxonomies, makes it difficult to understand the figures' accuracy fully. This is true not only across agencies, for example, The Cyber Helpline’s taxonomy versus crime codes within policing, but within agencies themselves. For example, there are variations in how one

crime might be categorised by different officers[6] . For instance, the Suzy Lamplugh Trust[32] found that incidents of stalking were often classified as malicious communications or assault. Likewise, The Cyber Helpline's chatbot diagnoses each case, and a trained Threat Intelligence Analyst verifies each. However, interpretation and a lack of information a service user gives may lead to a misdiagnosis.

All sources of data are also prone to duplicate reports; for instance, someone may seek support from a Victim Support organisation multiple times or report the crime multiple times. This may be particularly true in stalking, as behaviours occurring within a stalking campaign are often treated as singular incidents[32] .

Furthermore, it is likely to be the case that there is a percentage of victims who are not represented in data from victim support organisations or policing. For instance, many may not recognise that they have experienced a crime, either due to not realising that anything has happened at all or not realising that what has happened is a criminal act[9] . Those from marginalised groups may face barriers not only preventing them from reporting the crime to the police but also from engaging with other services[33] .

Due to the lack of data available, submitting FOI requests to understand the number of stalking and harassment cases utilising technology was considered. However, the significant underutilisation of the 'cyber-flag'[6] made this counterproductive to addressing the true nature of stalking and harassment. For this reason, an informed assumption was made that 90% of cases of this nature involve technology to some extent. Whilst this highlights a need for improvement in recording cybercrime and online harms, this assumption is likely to lead to a level of inaccuracy in this data.

Recommendations

Develop a fit-for-purpose reporting system

The current model for reporting cybercrime and online harms in England and Wales is inadequate. Inconsistent ways of reporting leads to duplication, inconsistencies in classification and varying responses. Furthermore, with only 35.77% of victims reporting cybercrime and online harms to the police, compared to 78.94% across all crime types, the evidence seems to show that this, at least in part, is due to confusion by victims on where to report and the accessibility of reporting.

Victims of cybercrime and online harm report that their online confidence diminishes as a result of the harm;;n a scale of 1-10 just under one-third of participants rated the impact the incident had on their online confidence as 10. With Action Fraud primarily operating as an online reporting tool, it is unlikely to be accessible for those who may feel their devices are compromised and could be scared to even turn their device on. The alternative is a phone line but with a high proportion of calls being abandoned,this seems likely to contribute to low reporting rates.

> "The police have given me misinformation and advice. For example in 2020 to keep making new emails that aren't connected to me in anyway, i.e not to use my name or DOB. This has

only left a trail of emails for third parties to access and use fraudulently. Recently I was questioned by police staff for 1hour 30mins before they submitted an 'online report' and gave the incident to a local resolution team's officer to 'look into'.. I had to make a complaint about the police staff, followed by a complaint by the person who handled the complaint and closed the case, followed by a complaint about the person who investigated his complaint. Only then was I given a crime reference."

Victim of Identity Theft

Learnings should be taken from other countries, including the Australian ReportCyber, who face similar problems to ActionFraud but at a reduced rate.

Online Confidence	
Empty	226
2	137
3	158
4	115
5	278
6	189
7	193
8	223
9	181
10 - very high	5
10	1001
1	553
Total	3259

Figure 5 - pivot table of responses to the question "How would you score the impact on your online confidence"

A fit-for-purpose reporting system would see a centralised, user-centric platform that integrates reporting channels into a single system and can transfer reports easily to the

relevant executive agency and/or police force. For accessibility purposes, reports on this platform should be able to be taken by police forces.

Victims should be offered real-time support in partnership with the third sector, providing signposting and referral opportunities to organisations such as The Cyber Helpline for immediate advice, assistance, and digital literacy information.

Information sharing with the private sector, such as banks, should be encouraged and automated where possible, to reduce delays, ensure the relevant parties are involved and facilitate threat intelligence sharing.

Awareness should be at the forefront of a new reporting system, making the public aware of what to report and where to report to increase reporting rates across all demographics.

A fit-for-purpose reporting system benefits not only the public but all stakeholders involved in cybercrime prevention and response, ensuring that trends in crime are understood and therefore can be better investigated.

Revise current crime codes, taxonomy and definitions

The current crime codes, taxonomy and definitions surrounding cybercrime and online harm should be revised. At present classifications are not representative of the complexity, overlap and evolving nature of cybercrime and online harms leading to varying interpretations of crime codes and, as a result, misclassification and an inaccurate representation of crime statistics.

A unified taxonomy for cybercrime that extends into policing, legislation, the cybersecurity industry and the victim support sector should be adopted for consistency in recording, reporting and processes for supporting victims. This should be integrated into crime codes to improve the accuracy of statistics.

The Cyber Helpline proposes a Human Attack Framework, similar to that of the MITRE ATT&CK framework, which classifies cybercrime against enterprises; this would allow consideration of overlaps of symptoms in providing a diagnosis and potential escalation pathways or evidence collection recommendations.

Revisit and standardise the ‘cyber flag’

The inconsistent usage of the ‘cyber flag’ across and within police forces undermines the ability to fully understand cybercrime, leading to underfunding or lack of priority in addressing these crimes through policy and policing.

Clear guidelines should be issued on the usage of the ‘cyber flag’ to police forces and crime recording bodies accompanied by mandatory training and incorporation into the National Crime Recording Standards to formalise usage. Its usage should be audited and monitored to ensure compliance and identify areas where it is not utilised correctly.

Enhance dedicated capacity for policing and investigating cybercrime and online harms

Limitations to policing cybercrime and online harms appear to include insufficient staffing, inadequate training and a lack of specialised resources preventing investigation. Academic studies, such as Curtis and Oxburgh[5] , have identified that resources are overstretched leading to delays in investigation or an entire lack of resolution.

Research[27] has also shown that officers do not understand how to handle cases involving cyber activity effectively, preventing them from providing effective advice and limiting the collection, analysis, and preservation of digital evidence. Officers are left to navigate the landscape of cybercrime and online harms and keep up to date with threats whilst being aware that their knowledge is limited and also needing to keep up to date with other crime types that they are dealing with day-to-day. For this reason, dedicated capacity must be available for cybercrime and online harms.

Every police force in the UK now has a dedicated cybercrime unit[34] ; however, little has been published on their work and scope. In 2023, the Metropolitan Police[35] stated in a Freedom of Information request that eighty staff members were employed in their Cybercrime Unit, yet over 30,000 officers are employed within the Metropolitan Police[36] in total. The existence of these units does not appear to translate into the capacity needed to handle the scale of cybercrime and online harms. This imbalance in the largest force in the UK shows the extent of under-resourced policing in cybercrime and online harms relative to the scale of the problem.

Funding and staffing within cybercrime units need to be increased, or consideration should be given to a national cybercrime and online harms unit that is equipped to deal with the unique challenges these cases present. Responding officers are expected to possess expertise in every type of crime, including cybercrime. However, given the specialised knowledge required to effectively manage, investigate, and respond to cybercrime and online harms, dedicated cybercrime units, including responding officers, are vital to enhancing digital investigations at all levels.

> “lost contact with society and feeling vulnerable, police only sending PCSO’s… they don’t understand technology as much as I do “
>
> Victim of Ransomware

Improve training, education and resources within the criminal justice system

A common theme throughout this report is the lack of knowledge on handling cybercrime and online harm within police forces. Training is vital if non-specialist officers are expected to continue to respond to and investigate cybercrimes and online harms.

The likelihood is that first responders to these crimes will be frontline officers. Research has shown that advice given by first responding officers may be to 'block them' or to delete online accounts[37] . This puts the onus on the victim and leads to a loss of evidence and potential use of other methods and escalations in perpetrators' behaviour, specifically in cyberstalking[38,39].

> "They think I should "just block them". But what they don't understand is that this person knows me and this will only anger them. Everytime I block them they get more invasive and more demanding. They get angry when I block and ignore them. It hasn't stopped me from doing so but it's not as simple as "just block them". I've been blocking him everywhere he tries to add/contact me for 4 months and now he's uploaded it to a website in retaliation."
>
> Victim of Intimate Image Abuse

Responding officers should not be expected to know everything about cyber, and specialised officers should exist to deal with these crimes but ultimately, with a majority of crimes involving at least some element of cyber frontline officers would benefit from better guidance in handling these cases, and this needs to be easily accessible.

However, different levels of training are needed for various roles within policing and the criminal justice system as a whole to ensure, for example, that:

- Frontline officers are equipped with essential cybercrime awareness and digital evidence handling;
- Specialised units have advanced knowledge in their areas;
- Prosecutors and judges are able to understand the technical aspects of cases that they will handle.

For example, The Cyber Helpline's Cyberstalking Action Plan has been adopted by several forces in the UK; however, in our experience, this training is often only commissioned for officers who are working in specialised roles and may not come into contact with the victim until much later in their reporting journey.

This training should come from collaboration with academia and industry experts ensuring that the latest evidence-based research and practice inform the training. Those working in the criminal justice system should also engage in regular CPD sessions to stay up to date with threats and trends in the rapidly evolving nature of cybercrime.

Training should also be standardised across the UK to ensure consistency in case quality and encourage information sharing amongst the criminal justice system.

Enhance multi-agency collaboration and communication

Cybercrime and online harm is multifaceted, requiring different areas of expertise and support. The justice system is only one area that victims can access, but it is potentially the only one they are aware of. Taylor-Dunn et al.[40] believe that police training should "shift the focus of the investigation from the behaviour of the offender, to the emotional impact on the victim.". Whilst police should be aware and informed of the impact of cybercrimes and online harm, the justice system is ultimately responsible for retribution. Nonetheless, police officers and others in the criminal justice system should be able to redirect victims to support which will help them in regaining their sense of safety online and offline, recovering lost funds or data, or feeling empowered to take steps to recover from the mental health impact of the crime. Those who come into contact with victims should feel able to ensure that they are aware of the resources and support that they can access to benefit their individual needs and wants.

Charities can provide support and should be working together to deliver information to victims, where consent is given to do so, aiming for a holistic approach for victims who may feel they are having to tell their story over and over and getting similar or even contradicting information, from various agencies who may be supporting their emotional health, physical safety, cybersecurity, advocacy and more. A multi-agency approach to cybercrime and online harms is vital for victim protection and wellbeing and maximising investigative opportunities.

Partnerships that allow for data sharing, particularly threat intelligence, between entities, would be a further beneficial opportunity; by sharing information on trends and threats as entities become aware of them, other organisations can be prepared to deal with the same or similar.

As an example, the Cyber Security Information Sharing Partnership exists in the UK to provide information sharing amongst the public and private sectors regarding cyber threats. However, they focus on supporting businesses rather than individuals. A similar model could be utilised, or the same model expanded, to enhance knowledge amongst those coming into contact with individual victims of cybercrime and online harms.

Victim-centric and evidence-based

Regaining public confidence in the policing of cybercrime and online harms, increasing reporting rates and retaining victims through the criminal justice process relies on an approach to policing that considers the wellbeing of the victim and proportionate and evidence-based actions.

With victims of cybercrime and online harm often experiencing long-term psychological impacts and immediate reduced quality of life[41] , the initial response to reports of cybercrime is vital to ensuring victims feel able to begin and continue the process of reporting and gaining a sense of justice. Victims need specialised support, which is distinct from traditional crimes. For example, McGuire and Dowling[9] show critical differences between online and offline crimes, including the relationship between the victim and perpetrator and the large

and global scale on which the crime may be operating. Even if the crime cannot be prosecuted, victims want to feel understood, believed and heard; they want to feel supported in navigating the complexities of cybercrime reporting and recovery; and provided with resources to regain their online confidence. Services should be accessible and inclusive, catering to unique needs, wants and perceptions of justice for each individual victim.

> “I feel partly safe because the police have reassured me that if anything happens I’m to ring 999 and an officer will be here immediately”
>
> Victim of stalking

The literature reviewed throughout this report has shown that analysing data from cybercrime is essential to understanding offending patterns, allocating resources effectively and understanding best practices to achieve the best possible outcome for victims. Evidence-based policing of cybercrime should be at the heart of evolving the approach to cybercrime, helping achieve consistency amongst cases and improving victim satisfaction and case outcomes. However, the College of Policing's What Works Toolkit for Crime Reduction fails to provide any interventions for cybercrimes and online harms; there is a lack of filters for digital crimes, and searching for relevant terms such as 'cybercrime', 'cyber', 'online' and 'digital' fail to return any results[42] showing that the evidence-base for policing cybercrime is either lacking, or not readily available to access and, therefore, not achieving its promise of encouraging consistent case handling.

The College of Policing[43] Practice Bank shows initiatives which different forces and organisations have implemented; this appears to show better results, with 14 other initiatives displayed when filtered by the topic of "Cybercrime including fraud", a majority - 57.14% - of these initiatives are based around prevention focusing on education, primarily for children; support for young victims and their families impacted by cybercrime and looking at hot-spots where types of cybercrime occur. Others look at improving the organisational handling of these cases including initiatives such as a Digital Advisory Network implemented by Durham Constabulary in 2021 to support officers in handling digital cases by having a point-of-contact for support. However, there is no published evaluation of this initiative.

There may be initiatives with no publicly available material, so it cannot be assumed these are the only initiatives in place. However, unique approaches to cybercrime and online harms across forces need to be empirically analysed to improve victim satisfaction, achieve positive outcomes through the criminal justice system and increase officers' confidence in case handling. These results must be available across forces, with forces provided with the resources to implement positive initiatives.

Where does The Cyber Helpline fit?

The Cyber Helpline supports over 100,000 individuals every year across the world; our data, insights and grounding in cybersecurity provide us with a unique, victim-first and

technology-led perspective on the cybercrime and online harm landscape. Our history puts us in a unique space to create a world where cybercriminals don't win.

Improving reporting rates and quality

The Cyber Helpline plays a role in addressing this issue; through our chatbot and helpline, victims are assisted through the complexities of the reporting process and submitting them to the appropriate agency.

In addition, The Cyber Helpline plays a role in improving the quality of reports by helping the individual understand what has happened and obtaining meaningful evidence, thus enhancing the quality of police investigations and potential outcomes. In the long term, this is beneficial not only for individual cases but in increasing the accuracy of data, strengthening arguments for the allocation of resources and informed policy decision-making, contributing to the long-term national strategy.

Training

The Cyber Helpline provides specialist training and resources for police forces and other stakeholders, focusing on practical guidance in supporting victims and managing evidence. Real-world scenarios and comprehensive data are integrated into the training to provide evidence-based best practices, better equipping those who come into contact with victims of cybercrime with confidence and dignity.

By providing this comprehensive training, the influence extends beyond victim interactions and awareness of these crimes' psychological and emotional impact. The training also offers the opportunity to improve investigations and, as a result, prosecution rates.

Taxonomy

The Cyber Helpline's unique data and insights provide us with an in-depth understanding of the current threat landscape, and the awareness of our service is only growing, providing us with the ability to understand how we can adapt to the evolving threats. The Cyber Helpline has already made developments in this area, developing a taxonomy that encompasses different types of cybercrime and online harms, allowing us to diagnose cases accurately and provide tailored support.

However, we recognise the need for a more comprehensive framework and aim to expand this taxonomy further, capturing the nuances of new and emerging cyber threats and the variances in attacks of the same or similar nature. We envision a taxonomy that captures and considers factors such as impact,victim-perpetrator relationship, cross-border complexities and motivations which integrates insights from technical practices and victim-centred perspectives. Ultimately, this will create a holistic tool that benefits policymakers, law enforcement, and victim support services by standardising approaches to classification.

This vision requires resources and investment but represents an opportunity for stakeholders to play a vital role in shaping a more accurate and adaptive understanding of the landscape, leading to better outcomes for victims.

Victim support and the Victims Code

Cybercrime has a violent impact on the individuals it impacts. The Cyber Helpline recognises the importance of addressing all impacts; our immediate support from cybersecurity expertise provides individuals with a lifeline. The lack of understanding of what has happened, how to report the crime, gather evidence and regain their online safety is often a barrier to receiving further support - being able to speak to someone who understands the technical elements of the crime is vital to achieving a resolution and sense of justice.

Feedback from service users highlights the importance of an advocate who understands the technical and emotional challenges involved. Our team of volunteers and staff work closely with victims to provide ongoing support and help them navigate complex issues, ensuring they do not feel alone in their journey at a time when they are likely to feel isolated.

In HMIC's[22] study of digital crime, a quote from a victim of cybercrime was provided: "They gave good advice, like asking me if there was anyone in my network that I could ask further IT advice from.". This raises the question of what happens if a victim doesn't have anyone from whom they can seek further advice. What happens if the advice given removes evidence or compromises the victim's physical safety? This is where The Cyber Helpline steps in.

Many victims of cybercrime feel their needs are unmet under the current system. Leukfeld et al.[44] found that cybercrime victims wanted regular updates during the investigative process and wanted to tell their stories and have their experiences recognised. These wants are reflected in the Victims' Code[45] ; our work aligns closely with this, allowing us to act as advocates and positioning us as a crucial partner in ensuring that victims of cybercrime receive the support they need, want and deserve.

The need for this support becomes increasingly urgent as threats continue to develop, yet providing and developing this level of support requires sustainable funding and resources. In our last financial year, however, we achieved a cost per case of just £11 - demonstrating our ability to help a large number of people at scale for little cost through the power of our volunteer-led model.

> “Reassured me that help was available. Kept me calm. The whole incident has been frightening. I am now feeling more myself. I have started researching for my PhD. I am eating in the kitchen and not the attic. I am no longer under his/her/their power.”
>
> Feedback from a victim of stalking

Conclusion

This report has highlighted significant gaps in reporting, investigation and prosecution meaning that victims of cybercrime are disproportionately less likely to achieve formal justice than those impacted by offline crimes.

A key issue is the gap between the scale of cybercrime and online harms and the resources dedicated to it within the justice system. With almost 60% of crimes in England and Wales now involving a digital element and seven times less likely to result in a charge or summons than offline crimes, the imbalance is evident. By examining the current limitations, it is possible to see how the UK has missed the need for more support in these crimes - from the inconsistent use of the 'cyber flag' to the barriers that prevent victims from reporting in the first place, the true nature and prevalence of cybercrime and online harms is masked.

This is only complicated further by the issues of taxonomy and classification. With current frameworks failing to capture the types of cybercrimes and online harms being experienced, without considering the overlaps inherent in these crimes, misclassification has likely led to missed opportunities for prioritisation of these crimes. As a result, this report has provided several recommendations, including a new, unified cybercrime and online harm taxonomy that supports accurate data collection and, ultimately, can guide policy and resource allocation.

To create a UK where cybercriminals don't win, a multifaceted approach that encompasses increased capacity in policing, improvement of training and resources for those in the criminal justice system, and revised reporting systems is essential for closing gaps in the funnel of justice. This can only be achieved through multi-agency collaboration between the justice system, victim support services and the private sector to ensure a holistic support system for victims, effective data sharing and advancing evidence-based best practices.

By addressing the issues identified in this report, the UK can create a justice system that better serves those impacted by cybercrime and online harm. The effort involved requires investment and collaboration but is crucial to ensuring that victims of cybercrime and online harm have access to the justice they need, want and deserve.

Bibliography

1. Crown Prosecution Service (2023) *Computer Misuse Act*. Available at: https://www.cps.gov.uk/legal-guidance/computer-misuse-act (Accessed: 12 May 2024).
2. Office for National Statistics (2024) *Crime in England and Wales: Year ending December 2023*. Available at:

https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2023#(Accessed: 12 June 2024).

3. York and North Yorkshire Police and Crime Commissioner (2022) *2022/23 Police precept*, *York & North Yorkshire Office for Policing, Fire, Crime and Commissioning*. Available at: https://www.northyorkshire-pfcc.gov.uk/police-oversight/finances/precept/2022-2023-police-precept/ (Accessed: 30 July 2024).
4. Sussex Police (2023) 'FOI Report: 3627/23 – Stalking Protection Orders'. Available at: https://www.sussex.police.uk/SysSiteAssets/foi-media/sussex/other_information/foi.3627.23-stalking_protection_orders.pdf.
5. Curtis, J. and Oxburgh, G. (2023) 'Understanding cybercrime in "real world" policing and law enforcement', *The Police Journal: Theory, Practice and Principles*, 96(4), pp. 573–592. Available at: https://doi.org/10.1177/0032258X221107584.
6. Office for Statistics Regulation (2024) *The quality of police recorded crime statistics for England and Wales*, *Office for Statistics Regulation*. Available at: https://osr.statisticsauthority.gov.uk/publication/the-quality-of-police-recorded-crime-statistics-for-england-and-wales/ (Accessed: 10 September 2024).
7. Laville, S. (2016) 'Internet used in eight cases of child sex abuse every day, NSPCC finds', *The Guardian*, 20 June. Available at: https://www.theguardian.com/society/2016/jun/21/internet-used-in-eight-cases-of-child-sex-abuse-every-day-nspcc-finds (Accessed: 13 May 2024).
8. Home Office (2023a) *Crime outcomes in England and Wales 2022 to 2023*, *GOV.UK*. Available at: https://www.gov.uk/government/statistics/crime-outcomes-in-england-and-wales-2022-to-2023/crime-outcomes-in-england-and-wales-2022-to-2023 (Accessed: 11 May 2024).
9. McGuire, M. and Dowling, S. (2023) *Cyber crime: A review of the evidence*. [online] Home Office. Available at: <https://assets.publishing.service.gov.uk/media/5a7caa0340f0b65b3de0a624/horr75-chap4.pdf> (Accessed 7 May 2024).
10. Phillips, K., Davidson, J.C., Farr, R.R., Burkhardt, C., Caneppele, S. and Aiken, M.P., 2022. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences, [online] 2(2), pp.379–398. https://doi.org/10.3390/forensicsci2020028.
11. Button, M. and Cross, C. (2017) *Cyber Frauds, Scams and their Victims*. London: Routledge. Available at: https://doi.org/10.4324/9781315679877.

12. Action Fraud (2024a) *Fraud and cyber crime national statistics*. Available at: https://www.actionfraud.police.uk/data (Accessed: 11 May 2024).
13. Suzy Lamplugh Trust (2021) *Unmasking Stalking*. Available at: https://www.suzylamplugh.org/Handlers/Download.ashx?IDMF=fcfb781a-f614-48c8-adcf-4cfa830c16a7.
14. Office for National Statistics (2023) 'Other related tables - year ending June 2023'. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesotherrelatedtables(Accessed: 13 June 2024).
15. Suzy Lamplugh Trust (2023) *Press Release: Research into Stalking Victims' Experiences of the CPS, HMCTS, and the Judiciary*, *Suzy Lamplugh Trust*. Available at: https://www.suzylamplugh.org/news/press-release-stalking-victims-experiences-of-the-cps-hmcts-and-the-judiciary (Accessed: 13 June 2024).
16. HM Government (2023) 'Fraud Strategy: Stopping Scams and Protecting the Public'. Available at: https://assets.publishing.service.gov.uk/media/64539087faf4aa0012e132cb/Fraud_Strategy_2023.pdf (Accessed: 30 July 2024).
17. Home Office (2023b) *Fraud Strategy: stopping scams and protecting the public (accessible)*, *GOV.UK*. Available at: https://www.gov.uk/government/publications/fraud-strategy/fraud-strategy-stopping-scams-and-protecting-the-public(Accessed: 23 June 2024).
18. Bowles, R., Garcia Reyes, M. and Garoupa, N. (2009) 'Crime Reporting Decisions and the Costs of Crime', *European Journal on Criminal Policy and Research*, 15(4), pp. 365–377. Available at: https://doi.org/10.1007/s10610-009-9109-8.
19. Böhme, R. (2013) *The Economics of Information Security and Privacy*. Berlin, Heidelberg: Springer. Available at: https://doi.org/10.1007/978-3-642-39498-0.
20. Sikra, J., Renaud, K.V. and Thomas, D.R. (2023) 'UK Cybercrime, Victims and Reporting: A Systematic Review'. Available at: https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/s3fs-public/2023-03/D19156-CCJ-1-1-UK-Cybercrime-Victims-Reporting--Sikra-et-al.pdf (Accessed: 30 July 2024).
21. Correia, S. (2021) 'Cybercrime Victims: Victim Policy through a Vulnerability Lens'. Rochester, NY. Available at: https://doi.org/10.2139/ssrn.3897927.

22. HMIC (2015) ‘Real Lives, Real Crimes: A study of digital crime and policing’. Available at: https://assets-hmicfrs.justiceinspectorates.gov.uk/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf.

23. Boyce, C.J. and Wood, A.M. (2010) ‘Money or mental health: the cost of alleviating psychological distress with monetary compensation versus psychological therapy’, *Health Economics, Policy and Law*, 5(4), pp. 509–516. Available at: https://doi.org/10.1017/S1744133109990326.

24. Human Rights Campaign Foundation (2023) *The Epidemic of Violence Against the Transgender and Gender Non-Conforming Community in the United States - HRC Digital Reports*. Available at: https://reports.hrc.org/an-epidemic-of-violence-2023 (Accessed: 8 September 2024).

25. Ikeda, S. (2021) ‘Disadvantaged Groups More Likely to Experience Cybercrime, Experience Disproportionately Damaging Results’, *CPO Magazine*, 11 October. Available at: https://www.cpomagazine.com/cyber-security/disadvantaged-groups-more-likely-to-experience-cybercrime-experience-disproportionately-damaging-results/(Accessed: 8 September 2024).

26. Action Fraud (2024b) *NFIB Dashboard (Public)*. Available at: https://colp.maps.arcgis.com/apps/dashboards/0334150e430449cf8ac917e347897d46 (Accessed: 11 May 2024).

27. Hadlington, L. *et al*. (2021) ‘A Qualitative Exploration of Police Officers’ Experiences, Challenges, and Perceptions of Cybercrime’, *Policing: A Journal of Policy and Practice*, 15(1), pp. 34–43. Available at: https://doi.org/10.1093/police/pay090.

28. Schreuders, ZC., Cockcroft, T., Butterfield, E., Elliott, J., Shan-A-Khuda, M. and Soobhany, A.R., 2020. Needs Assessment of Cybercrime and Digital Evidence in a UK Police Force. [online] https://doi.org/10.5281/ZENODO.3757271.

29. Bossler, A. *et al*. (2020) ‘Policing fraud in England and Wales: examining constables’ and sergeants’ online fraud preparedness’, *Security Journal*, 33(2), pp. 311–328.

30. *Online Safety Act 2023* (c.50) [online] Available at: https://www.legislation.gov.uk/ukpga/2023/50 [Accessed 31st July 2024].

31. Voce, I., and Morgan, A.(2023) Cybercrime in Australia 2023. Statistical Report no. 43. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sr77031

32. Suzy Lamplugh Trust (2022) ‘Super-complaint on the police response to stalking’. Available at:

https://www.suzylamplugh.org/Handlers/Download.ashx?IDMF=cf3fdc8b-f958-4cc0-9fc7-9ce6de3e9137 (Accessed: 10 September 2024).

33. Victim Support Europe (n.d) 'Marginalised Victims'. Available at: https://victim-support.eu/help-for-victims/info-on-specific-types-of-victims/marginalised-victims/ (Accessed: 10 September 2024).
34. NPCC (2019) *Dedicated Cybercrime Units Get Million Pound Cash Injection, National Police Chiefs' Council (NPCC)*. Available at: https://news.npcc.police.uk/releases/dedicated-cybercrime-units-get-million-pound-cash-injection(Accessed: 12 September 2024).
35. Metropolitan Police (2023) *Staff and money spent on Cybercrime department*. Available at: https://www.met.police.uk/foi-ai/metropolitan-police/disclosure-2023/november-2023/staff-money-spent-cybercrime-department/ (Accessed: 29 July 2024).
36. Metropolitan Police (n.d.) *The structure of the Met and its personnel*. Available at: https://www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/structure/ (Accessed: 17 September 2024).
37. Black, A., Lumsden, K. and Hadlington, L. (2019) '"Why Don't You Block Them?" Police Officers' Constructions of the Ideal Victim When Responding to Reports of Interpersonal Cybercrime', *In: LUMSDEN, Karen and HARMER, Emily, (eds.) Online Othering. Palgrave Studies in Cybercrime and Cybersecurity . Springer International Publishing*, pp. 355–378.
38. Eterovic-Sorc, B., Choo, KKR., Ashman, H., Mubarak, S. (2017) 'Stalking the stalkers – detecting and deterring stalking behaviours using technology: A review', *Computers & Security*, 70, pp. 278–289.
39. Sussex Police & Crime Commissioner (2020) *'Mute, don't block your stalker'*. Available at: https://www.sussex-pcc.gov.uk/about/news/mute-don-t-block-your-stalker/ (Accessed: 22 September 2024).
40. Taylor-Dunn, H., Bowen, E. and Gilchrist, E.A. (2021) 'Reporting Harassment and Stalking to the Police: A Qualitative Study of Victims' Experiences', *Journal of Interpersonal Violence*, 36(11–12), pp. NP5965–NP5992. Available at: https://doi.org/10.1177/0886260518811423.
41. Ignatuschtschenko, E. (2021) 'Assessing Harm From Cyber Crime', in Cornish, P., *The Oxford Handbook of Cyber Security*. Oxford University Press, pp. 127–143.

42. College of Policing (2024a) *Crime reduction toolkit*. Available at: https://www.college.police.uk/research/crime-reduction-toolkit (Accessed: 4 October 2024).

43. College of Policing (2024b) *Practice bank*. Available at: https://www.college.police.uk/support-forces/practices (Accessed: 4 October 2024).

44. Leukfeldt, E.R., Notté, R.J. (Raoul) and Malsch, M. (Marijke) (2020) 'Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes', *Victims & Offenders*, 15(1), pp. 60–77. Available at: https://doi.org/10.1080/15564886.2019.1672229.

45. Ministry of Justice (2024) *Code of Practice for Victims of Crime in England and Wales (Victims' Code)*, *GOV.UK*. Available at: https://www.gov.uk/government/publications/the-code-of-practice-for-victims-of-crime/code-of-practice-for-victims-of-crime-in-england-and-wales-victims-code (Accessed: 16 October 2024).