

# The Swansea Cyber Clinic Project: A Stakeholder Report

---

Sara Correia-Hopkins and Janet Oostendorp Godfrey

AUGUST 2023

# CONTENTS

<b>01.</b>	Key Takeaways	p. 3
<b>02.</b>	Introduction	p. 4
<b>03.</b>	Aims & Methodology	p. 5
<b>04.</b>	What We Learnt	p. 6
<b>05.</b>	Recommendations	p. 11
<b>06.</b>	Useful Resources	p. 12
<b>07.</b>	Annex A: Victim Support Toolkit	p. 13
<b>08.</b>	References	p. 15



Hillary Rodham Clinton  
School of Law | Ysgol y Gyfraith

# KEY TAKEAWAYS

- 01** **Crime is 'hybrid'.**  
In a 'digital' society, crime and victimisation are increasingly online/offline 'hybrids', creating challenges and opportunities for victim responses.
- 02** **There are strengths and gaps in victim support provision.**  
Mapping victims' needs to existing services revealed strengths (e.g., around partnership working), but also gaps in victim support provision, barriers to access and challenges for practitioners. This includes limited technical support, as demonstrated by our [Service Mapping](#) tool. It also includes negative perceptions of policing and victim expectations.
- 03** **Resources are limited and stakeholder networks are essential to meet victims' needs.**  
Practitioners across sectors highlighted issues of limited resourcing but also issues of policy ownership and clarity of expectations around what and how victims' needs should be addressed. Many stakeholders are involved in supporting victims and services vary across time and geographic area. Investing in building strong networks of local support is therefore vital.
- 04** **Our 5 principles to improve response for victims:**
- Victim voice and participation at the centre of the response;
  - Develop a Needs & Vulnerability Assessment;
  - Prioritise protection from re-victimisation and securing evidence.
  - Encourage partnership working across national, local, generalist and specialist services;
  - When developing new tools and initiatives, consider holistic and accessible support, recognising digital and other inequalities.
- 05** **Our 10 recommendations:**  
On page 11, we make final our recommendations drawing on these principles.

# INTRODUCTION

*"But it's also not ok for someone to do this to someone and get away with it. You know it was constant, you know. And it was all made to intimidate me and scare me, and I just think, I feel he is going to get away with it and there's nothing I can do."*

**Interviewee 2**

One in ten people are estimated to become victims of online crime every day, including online fraud, romance fraud, sexual extortion, public or private threats, stalking and harassment, hate crimes and other malicious communications (Victim Support, 2022). In today's digital society, crime and victimisation are increasingly 'hybrid,' meaning that online and offline elements are mutually reinforcing and cannot be separated. Victims themselves are often a hybrid of multiple agents, including 'real' humans and 'virtual' machines (van der Wagen & Pieters, 2015, 2020).

*The National Fraud Intelligence Bureau received 372,194 reports of cybercrime in the 12 months to May 2023, 88% were from individuals (NFIB 2023)*

With the development of cybercrime as a service within criminal networks, the same hybridity can characterise perpetrators. Nonetheless, the criminal justice system's (CJS) response to crime is still split between 'cyber' and 'the rest', where the former is perceived as less of a priority (Button et al., 2022). Given its prevalence however, there is a danger that lack of action on 'cyber' and/or 'hybrid' crimes will fuel a negative cycle of under-reporting and lack of trust in police forces.

For example, the Office for National Statistics (ONS) estimates that there were 936,276 incidents of fraud (over half of which took place online) and 28,886 incidents of Computer Misuse (CM) in England and Wales in 2021 (ONS, 2022). However, only 14% of fraud and 4% of computer misuse incidents were reported to the police in the year ending March 2022 (ONS, 2022). Of these thousands of reports made to law enforcement, only 3% of fraud and 15% of computer misuse reports were included in disseminations for investigation under the 'Pursue' response, with the majority of these being closed with no suspect identified (Home Office, 2022). These data raise the question of whether practitioners and victims perceive current attempts to investigate, prevent and protect victims from hybrid crimes are adequate.

*Only 14% of fraud and 4% of computer misuse incidents were reported to the police in the year ending March 2022 (ONS 2022)*

However, limited research has been undertaken into how law enforcement, victim support networks and services are evolving to support victims of hybrid crimes and how they are coping with the challenges of an increasingly digital society. In this context, it is timely to listen to stakeholders and victims to (re)consider what a meaningful response to hybrid crime and victimisation should look like.

*"She's had some real attitude problems from the Police, you know, the officers that she's spoken to have gone, 'What's their issue? What's the problem? We don't see... there's no problem here, there's no laws broken, what are you on about? And that's their attitude."*

**Interviewee 3**

# AIMS & METHODOLOGY

## Research Aims

The aims of this research were to:

1. Explore the extent to which victim services are adequate in a 'Digital Society' and
2. Develop ideas for new strategies, services and tools, to help better understand and increase individuals' resilience to victimisation.

## Methodology

The Swansea Cyber Clinic was a qualitative pilot co-design project, undertaken between August 2021 and July 2022, by researchers in law and computer science at Swansea University, in collaboration with South Wales Police and the Swansea Council for Voluntary Services. This project was funded through a 'Basecamp' award from Swansea University's Morgan Advanced Studies Institute (MASI).

### Sample

25 practitioners and 3 victims, based within the southern Wales Police force areas (including Dyfed/Powys, Gwent and South Wales) took part in this research.

Role	N	Experience (mean years)
Industry	3	9.83
Law Enforcement	11	8.18
Public Sector	4	8.33
Third Sector	7	5.29

The research followed five stages:

1. A project Advisory Group was established, including professionals with experience of supporting victims, or relevant expertise (see acknowledgements).
2. Desk-based research was undertaken to map the current support available to victims of hybrid crimes in Wales. This was updated throughout the project, as services were mentioned by participants.
3. Six focus groups were undertaken with 25 victim support practitioners. These were used to reflect upon and refine the service mapping data, as well as to explore practitioners' experiences of providing support to victims.
4. Interviews with 3 victims were undertaken to explore personal experiences of victimisation and support and to develop three illustrative case studies.
5. Two workshops were run with 12 stakeholders and software developers, using the 'Disney method' as a creative strategy (see references on p.15). These workshops enhanced the ideas for victim support services and tools, previously identified by focus group and interview participants.

### Limitations

- Subject to future updates, Service Mapping tool is limited to victim support services operating in Wales, within the research period.
- Given the self-selecting nature of our sample, these data are not representative of all practitioners or victims. However, as this project was exploratory, it captured a wide range of participant views, to identify gaps and ground a future research agenda. In addition, it benefited from continuous consultation with the project Advisory Group.
- Direct engagement with victims was limited. In particular, the prioritisation and co-design workshops were undertaken with practitioners and software engineers only. Nonetheless, this research provides powerful first-person accounts, with participants recruited across geographical areas, age groups, gender identity, and ethnicity.

# WHAT WE LEARNT

## What types of victimisation?

- The types of victimisation experiences identified by participants as hybrid included **Abusive Behaviour, Fraud, Computer Misuse** and 'Other'.
- There were 19 sub-categories found across these groups of which, those identified as having the greatest negative impact on victims by practitioners included a) **Sextortion & Image based Sexual Abuse**, b) **Stalking & Harassment**, c) **Romance Fraud** and d) **Domestic & Intimate Partner Abuse**.

## What is the impact on victims?

Practitioners identified a range of financial and non-financial impacts on victims (see Figure 1).

- **Financial losses** included **direct** losses, **indirect** debt, and **exclusion** from financial services, with repercussions for dependant family members and victims' own mental health.
- **Non-financial impacts** (see Box 1) were highlighted as the most significant by practitioners and victims, none more so than **emotional impact**.

## Who are the victims?

Victim profiles vary but practitioners identified some groups as posing specific challenges and opportunities, namely:

- Different needs were emphasised across age groups, including a differentiation between children and young people, middle-aged and elderly victims. Other important demographic factors highlighted included gender, disability and whether individuals live with health conditions.
- Other victim groups and characteristics highlighted included those who are lonely or isolated. In relation to occupations and organisations, practitioners discussed the needs of sole traders, micro and small enterprises, and sex workers.

*"For us it's a real mix. (...) I think a lot of people assume that it is the older generation that this type of thing happens to. However, we do get a lot of reports every week on social media hackings so, the younger generation, who sort of think, (...) oh I'm tech savvy. This is not gonna happen to me..."*

**Focus Group 3**

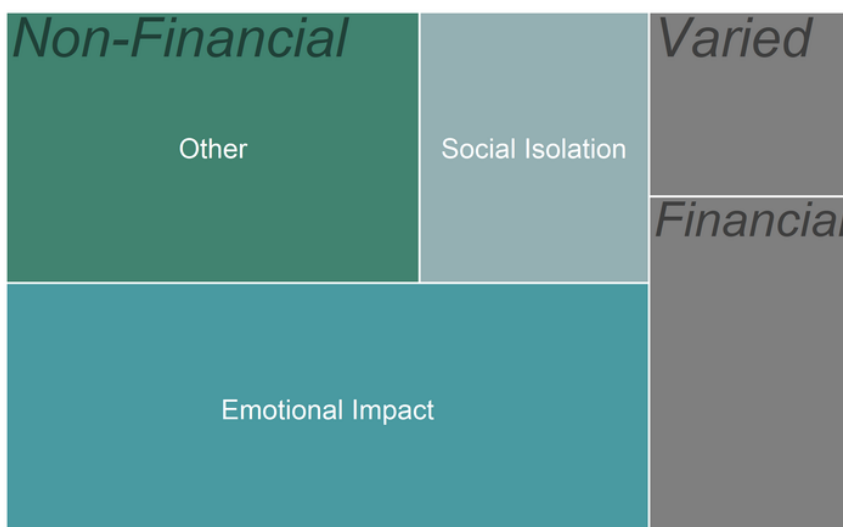


Figure 1 - Victim impacts discussed by practitioners. Size of boxes represent number of transcribed text items coded.

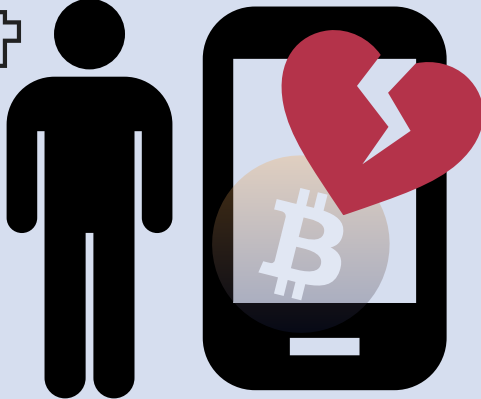
### Box 1 - Non-financial impacts.

- 1. Emotional Impact** includes feelings of embarrassment & shame, fear & vulnerability and shock & confusion;
- 2. Social Isolation** includes isolation resulting from victimisation adversely affecting victims' relationships with family & friends as well as a general decline in feelings of trust in others.
- 3. Other Impacts** includes a range of other impacts on health & confidence, being repeatedly victimised, concerns about personal liability, negative impacts of daily & family life, privacy intrusions, physical threats and suicidal feelings.

# VICTIM IMPACT CASE STUDIES

The following three vignettes are based on the victim interviews and highlight the extent of the the impact of hybrid crime.

**30-34**  
years




**Impact themes:**

- Direct Loss
- Embarrassment & Shame
- Mistrust in Others

"You know, falling in love with someone, and then getting to the find out that person is not who you thought the she was, that was a major loss. More than the financial loss. [...] Broken, [I felt] broken, especially after the love scam, broken."

"Well it gave me a panic attacks and which I've never had before. And real anxiety to the point where I had to go on medication and stuff and had to have some time off work. "



**30-34**  
years

**Impact themes:**

- Fear & Vulnerability
- Health & Confidence
- Mistrust in Others

**45-49**  
years



**Impact themes:**

- Fear & Vulnerability
- Health & Confidence
- Mistrust in Others

"I check under the car [for bombs] as a matter of fact. I got a mirror, that I stuck on a stealth selfie stick and I check the car underneath. Because we're in an open car park, where we are, so I check that daily. "

# VICTIM NEEDS

## What do victims need and expect?

- **Reassurance & Knowledge:** Including validation of their lived experience of victimisation, as well as support to understand what happened to them and how to proceed.
- **Protection:** Advice and tech support to enable victims to protect themselves from further victimisation.
- **Enforcement & Justice Outcome:** An enforcement response e.g., take downs and evidence collection, leading to an investigation and/or a criminal justice outcome.
- **Impact Recovery:** Support to recover from the financial and other impacts of victimisation

As illustrated in Figure 2, practitioners discussions in the focus groups focused on victim support responses, over and above an enforcement response or criminal investigation. Nonetheless, as the following excerpts highlight, a criminal justice outcome was an expectation highlighted in each of the following quotes from the interviews.

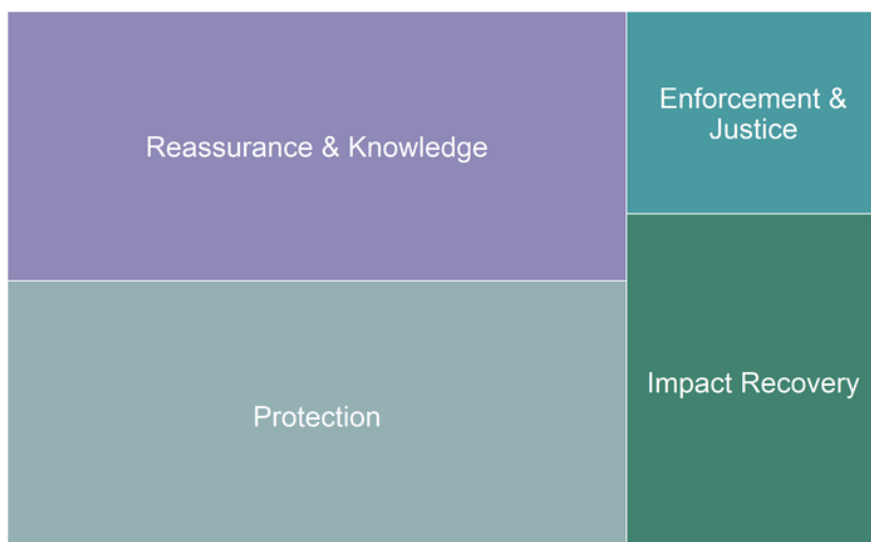


Figure 2 - Victim needs and expectations discussed by practitioners.

"[I expected] **swift action** by the law enforcement agencies, you know, to **get the culprit** and at least **get my money back**. You know, that was what I was expecting."

Interviewee 1

"[...] I only know nice people. So also I felt really passionate about it. I thought I've got to **catch this person** 'cause you know, who would do this to me? **I began to not trust so many people.**"

Interviewee 2

"Because those are the things that there is **a safety net**, they're there to help you and to make you feel secure and to know that if there is a serious incident, because it's only stepping up, it's only getting worse, it's not getting better is this... [nervous laughter] so **if there is a serious incident, then at least you haven't got to sit on a phone and wait** for it to be answered on 999, for a start, when it's an emergency. You know these guys are serious. It could be a real emergency..."

Interviewee 3

All three quotes above imply that an enforcement response was important to the victims, because they hoped it would lessen and/or enable them to cope with the impacts of victimisation, both financial and non-financial.

"[The victims] often don't have the full understanding of what they should do to protect themselves, so they're really looking for someone to come in and give them a road map of what they should do."

Focus Group 1



# BARRIERS & CHALLENGES

## What support is available and what are the barriers victims face when accessing this support?

This project identified a range of support which is currently available to victims of hybrid crimes.

Predominantly the current services and processes mirror the needs identified above. However, the most significant gaps identified, related to Protection – Tech Support and all aspects of Impact Recovery, especially as financial recovery is unlikely and Mental Health services over-subscribed.

Practitioners reflected that:

- Proactive crime prevention is an important element of the response to hybrid crime, as “prevention is better than cure”.
- Referral pathways between organisations are key to meet the wide range of victim needs, some of which require a specialised response.
- There are barriers to victims accessing existing support services including around perceptions, awareness & engagement and structural barriers (see Box 2).

### Box 2 - Barriers to Access

- 1. Perceptions:** Limited understandings of victims and what constitutes victimisation, under-estimations of the impact of ‘hybrid’ crimes, as well as of negative perceptions of criminal justice system agencies.
- 2. Awareness & Engagement:** Limited victim awareness of, and engagement with, the support that is available and/or provided.
- 3. Structural:** Wider structural socio-economic barriers, which get in the way of victims accessing the support which is available.

## What are the challenges when delivering victim-focused responses?

- **Resourcing & Capacity:** Low levels of resourcing result in limited response capacity for victim-facing services.
- **Victim Engagement:** Engaging victims and managing their expectations while catering for varied/complex needs.
- **Standards & Strategy:** Low response standards and lack of developed strategy/frameworks, focused on identifying and responding to victims’ needs.
- **Partnerships Working:** While partnership working across sectors was seen as key to the current victim support model, practitioners also identified that challenges arise from partnership working.
- **Skills & Training:** Staff development & keeping up with technical knowledge.
- **Enforcement:** Challenges arising from the global and anonymous nature of the internet.

*“I think ... you can kind of stretch yourself to meet more capacity and more volume, but it's the quality of the service that's provided [that will suffer]... you can kind of half heartedly investigate and support each victim, but if you have the resources there to give them the actual support and and the time to actually investigate things properly and not having to prioritize cases, you're going to get a lot more success. ”*

### Focus Group 3



Figure 3 - The challenges of delivery.

# IMPROVING VICTIM RESPONSE

## How do we improve the victim response?

*"I believe you have to work as a multi agency and I think that's what we will always go through with our victim ... you have to work with other organisations. If something is lacking on one side of it, go and see where you can get that with other support from."*

**Focus Group 6**

We identified five guiding principles for an improved support model:

- 1. Victim Voice & Participation:** Victim voice and participation should be imbedded wherever possible. This approach will contribute to addressing current barriers, victim needs and provide space for reflection and continuous service improvement.
- 2. Needs & Vulnerability Assessment:** Alongside victim voice, a response focused on victims needs inevitably requires that a needs & vulnerability assessment becomes central to a response framework.
- 3. Protecting People & Securing Evidence:** National and local strategies to address hybrid crime should be focused on protecting people from re-victimisation and securing (digital) evidence. A shift is needed away from 'Investigation' is impossible, towards more investigations, as well as 'Protection' and 'Healing' for victims.
- 4. Partnership Working:** A mix of national/local and generalist/specialist services, closely networked and working in partnership to common standards and strategic objectives is required. Collaboration should be encouraged, rather than competition.
- 5. Holistic & Accessible Support:** The response is holistic i.e., it goes beyond an incident-by-incident response and addresses the full range of victim needs. Support formats are varied and accessible, including anonymous self-help options.

## Victim Response Toolkit

It is useful to distinguish between pro-active responses, aimed at protection and prevention and re-active responses, designed to meet victims' needs once victimisation occurs. Focus group participants made **27 practical suggestions** for strategies and tools to help improve the proactive and reactive elements of victim responses. During the co-design workshop, participants ranked the tools in order of priority. The colour of the tiles in Figures 4a and 4b indicates the order of priority given from least (-4) to greatest (+12) priority. For the full list and descriptions, see Annex A.

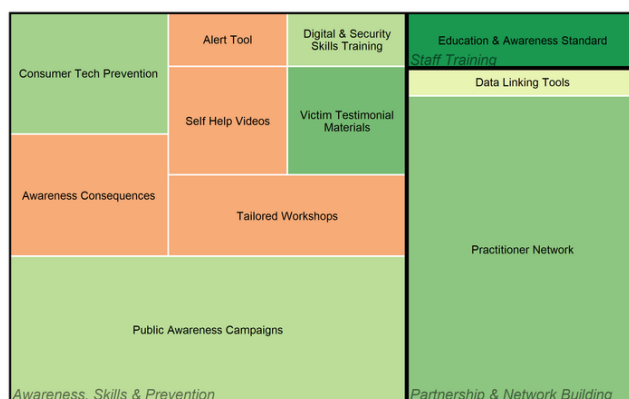


Figure 4a - Tools: Proactive Response.

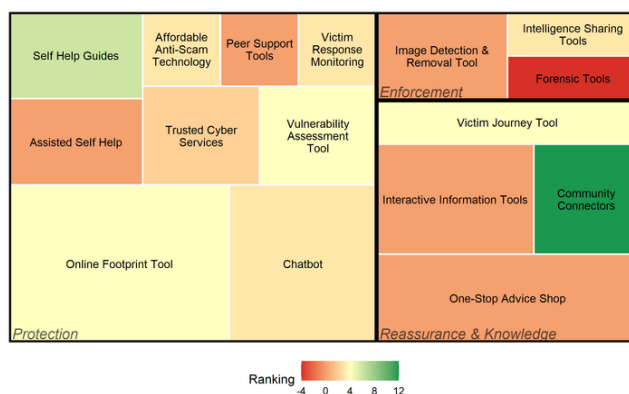


Figure 4b - Tools: Reactive Response.

At the workshops, participants were asked to consider which of these would best suit their expertise/experience and select tools for detailed discussion. The tools discussed in detail included the *Online Footprint Tool*, *Chatbot*, *Community Connectors*, *One-Stop Advice Shop* and a *Victim Journey Tool*.

# RECOMMENDATIONS

These recommendations will inform future work by the Swansea Cyber Clinic and partners:

01	Recognise that experiences of <b><u>victimisation and harm are increasingly 'hybrid'</u></b> , and that 'cyber' response skills are needed across the board.
02	<b><u>Victim voices</u></b> should be at the heart of the victims-focused responses and agencies should be proactive in seeking these.
03	A <b><u>needs &amp; vulnerability assessment</u></b> should be undertaken to ascertain how best to respond where individuals report hybrid victimisation to agencies. Prevention and protection support should be tailored, and sensitive to, groups with particular needs.
04	Crime <b><u>reporting processes</u></b> should be reviewed to ensure they <b><u>trigger adequate 'Protect'</u></b> responses where needed.
05	Develop tools and strategies to <b><u>evaluate 'what works'</u></b> in relation to 'Protect' responses.
06	<b><u>Restorative conversations</u></b> should be used to help victims process and articulate their needs and to ensure their expectations are aligned with the available/possible help.
07	Create and disseminate <b><u>opportunities for training</u></b> , both formal and informal, aimed at practitioners. This should encompass how to assess and respond to vulnerability and impact, across a variety of crimes and harms.
08	Establish a <b><u>network of practitioners</u></b> to help keep stakeholders in touch with victim needs, the available support and emerging threats.
09	<b><u>Knowledge sharing</u></b> between third sector, higher education and industry organisations, will help individuals develop awareness and skills to secure digital evidence and protect their digital footprints.
10	Any new (digital) <b><u>tools and services</u></b> to support victims should be developed following user-centred approaches, taking into account <b><u>digital and other inequalities</u></b> .

# USEFUL RESOURCES

## Report a Crime

- In an emergency call 999
- If you are experiencing a live cyber-attack, call 101
- If you suspect a cybercrime or fraud, contact Action Fraud on 0300 123 2040 or click to follow the link <https://www.actionfraud.police.uk/>

## Victim Support

- Victim Support provide advice across Wales, call them on 08 08 16 89 111, or click to follow the link <https://www.victimsupport.org.uk/>

## Security Advice & Support

- The CyberHelpline provides free anonymous self-help advice and 1-2-1 advice, from cyber-security experts or click to follow the link <https://victimadviceline.org.uk/specialist-service/the-cyber-helpline/>
- You can access useful guides and advice at the CyberAware website or click to follow the link <https://www.ncsc.gov.uk/cyberaware/home>

## Wellbeing & Mental Health

- For wellbeing and mental health support, contact Mind on 0300 123 3393 or click to follow the link <https://www.mind.org.uk/>

## Stalking Support

- Contact The National Stalking Helpline on 0808 802 0300 or click to follow the link <https://www.supportline.org.uk/problems/stalking-and-harassment/>

## Domestic & Sexual Abuse

- For support with domestic and sexual abuse, contact the Live Fear Free Helpline on 0808 80 10 800 or click to follow the link <https://www.gov.wales/live-fear-free>

## Support for children

- For support for children and young people (up to 19), contact Childline on 0800 1111 or click to follow the link [Contact the Live Fear Free Helpline on 0808 80 10 800 or click to follow the link https://www.gov.wales/live-fear-free](https://www.gov.wales/live-fear-free)

# ANNEX A: TOOLKIT

The table that follows provides a description for the tools suggested by practitioners to improve the **proactive victim response** i.e., victim protection and prevention.

Tool	Description
Alert Tool	An alert tool for businesses to get up to date a relevant information about cybercrime trends.
Awareness Consequences	Resources to make (young) people aware of the legal consequences of certain behaviours, especially re the sharing of indecent/private/sexual images.
Consumer Tech Prevention	Information packs to be sent out to individuals when purchasing consumer tech, with information about preventing (further) victimisation.
Data Linking Tools	Tools to enable agencies to link data on cyber and hybrid crimes to other relevant datasets e.g., other police recorded crimes.
Digital & Security Skills Training	Training to provide basic digital skills and security training to individuals.
Education & Awareness Standard	Develop a common standard and minimum provision for digital and cyber skills and awareness initiatives.
Practitioner Network	Establish a practitioners' network to enable victim support practitioners to be well networked and aware of other services and initiatives locally and nationally.
Public Awareness Campaigns	Public awareness campaigns to increase visibility of crime/harm with a view to preventing victimisation wherever possible e.g., TV adverts.
Self Help Videos	Step-by-step videos to help victims improve their security and awareness.
Tailored Workshops	Digital confidence and cyber security victim-training or workshops, tailored to specific populations.
Victim Testimonial Materials	Develop victim testimonial materials may to help communicate the full impact of cyber and hybrid crimes.

# ANNEX A: TOOLKIT

The table that follows provides a description for the tools suggested by practitioners to improve the **reactive victim response** i.e., to help meet victims' needs post-victimisation.

Tool	Description
Affordable Anti-Scam Technology	Develop anti-scam technology e.g., call blockers, which is more affordable, in order victims to prevent re-victimisation.
Assisted Self Help	Resources and tools to help victims to help themselves e.g., guides walking them through security settings, as a way to increase protection long term.
Chatbot	Using/improving existing chatbots to aid victims in accessing support and protection advice, in the context of a complex landscape of support.
Community Connectors	Individuals who know the community resources well and are able to link victims with the available support across a range of needs.
Footprint Tool	Tool to help capture and address risks linked to victims' online footprints.
Forensic Tools	Need for new/improved forensic tools.
Image Detection & Removal Tool	A tool used to detect image based sexual abuse through hashing technology, which will automatically flag/remove content to prevent its spread through the internet, etc.
Intelligence Sharing Tools	Tools to allow different agencies to quickly share information about new trends in cyber and hybrid crimes.
Interactive Info Tool	Interactive digital tool to enable victims to access the information they need and understand the next steps, regardless of whether crime was reported.
One-Stop Shop	A central resource which victims across the UK can be referred to, in order to understand what support is available and access self-help.
Peer Support Tool	Tool to enable victims to participate in peer support.
Self Help Guides	Guides to enable victims to check and secure own accounts and devices for malicious activity, to prevent further victimisation.
Trusted Cyber Services	A resource to enable victims and practitioners to identify trustworthy cyber security services, to which individuals can be referred.
Victim Journey Tool	A tool to show victims where their case is within the Criminal Justice System.
Victim Response Monitoring	Tools to help monitor the progress of cases and the support provided to victims.
Vulnerability Assessment Tool	Toolkit to assess vulnerability to specific hybrid crimes (e.g., fraud).

# REFERENCES

- Button, M., Shepherd, D., Blackburn, D., Sugiura, L., Kapend, R., & Wang, V. (2022). Assessing the seriousness of cybercrime: The case of computer misuse crime in the United Kingdom and the victims' perspective. *Criminology & Criminal Justice*. <https://doi.org/10.1177/17488958221128128>
- Home Office. (2022, July 21). Crime outcomes in England and Wales 2021 to 2022. <https://www.gov.uk/government/statistics/crime-outcomes-in-england-and-wales-2021-to-2022/crime-outcomes-in-england-and-wales-2021-to-2022#experimental-statistics-investigative-outcomes-assigned-to-fraud-and-computer-misuse-act-cma-offences>
- NFIB. (2023). NFIB Fraud and Cyber Crime Dashboard. <https://colp.maps.arcgis.com/apps/dashboards/0334150e430449cf8ac917e347897d46>
- ONS. (2022). Nature of fraud and computer misuse in England and Wales: Appendix tables—Year ending March 2022. Office for National Statistics. <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/natureoffraudandcomputermisuseinenglandandwalesappendixtables>
- Tausch, S., Steinberger, F., & Hußmann, H. (2015). Thinking Like Disney: Supporting the Disney Method Using Ambient Feedback Based on Group Performance (J. Abascal, S. Barbosa, M. Fetter, T. Gross, P. Palanque, & M. Winckler, Eds.; pp. 614–621). Springer International Publishing.
- van der Wagen, W., & Pieters, W. (2015). From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks. *British Journal of Criminology*, 55(3), 578–595. <https://doi.org/10.1093/bjc/azv009>
- van der Wagen, W., & Pieters, W. (2020). The hybrid victim: Reconceptualizing high-tech cyber victimization through actor-network theory. *European Journal of Criminology*, 17(4), 480–497. <https://doi.org/10.1177/1477370818812016>
- Victim Support. (2022, January). Cybercrime – how we can keep you safe online. [https://www.victimsupport.org.uk/wp-content/uploads/2020/11/P2714\\_12-Cyber-Crime-leaflet.pdf](https://www.victimsupport.org.uk/wp-content/uploads/2020/11/P2714_12-Cyber-Crime-leaflet.pdf)

# ACKNOWLEDGEMENTS

This project and report would not have happened without the invaluable contributions of each member of the multi-disciplinary research team, including, in no particular order: Dr Leigh Clark, Dr Martin Porcheron, Dr Nnenna Ifeanyi-Ajufo, Dr Stuart Nicholson and Ms Genevieve Clifford.

As a team, we are much indebted to all the members of the project Advisory Group, which provided much encouragement as well as the best critical friend feedback we could have hoped for. They included:

- Cadi Cliff (Cwmpass / Digital Communities Wales)
- Prof. Cassandra Cross (Queensland University of Technology)
- DS Chris Algar (South Wales Police)
- Hannah Lawson (Swansea Council for Voluntary Services)
- Jess Rees (Victim Support Wales)
- John Davies (Cyber Wales)
- DS Matthew Phillips (South Wales Police)
- Roxane Dacey (Swansea Council for Voluntary Services)
- DS Stephen Jones (South Wales Police)
- Dr Vasileios Karagiannopoulos (University of Portsmouth)
- Victoria Lloyd (AgeCymru)

The views expressed in this report are those of the authors and do not claim to represent those of the individuals mentioned above, or any of the institutional partners.

---

*Finally, we must thank Swansea University and in particular the Morgan Advanced Studies Institute (MASI), for providing the seed funding needed to kickstart this project and the Faculty of Humanities and Social Sciences for their subsequent support.*

---

## CONTACT

For further information about this report, please contact:  
[cyberclinic@swansea.ac.uk](mailto:cyberclinic@swansea.ac.uk)

HRC School of Law, Swansea University, Singleton Campus,  
Swansea, SA2 8PP