

Ireland Needs a National Cyber Security Helpline

Supporting people in Ireland affected by cyber incidents through compassionate support, trusted information and coordinated referrals.



NATIONAL
CHALLENGE
FUND

From Ingenuity
to Research
and Solutions



Rialtas na hÉireann
Government of Ireland

Taighde Éireann
Research Ireland



Maoinithe ag an
Aontas Eorpach
Funded by the
European Union
NextGenerationEU



MTU

Ollscoil Teicneolaíochta na Mumhan
Munster Technological University

Introduction

Ireland is becoming an increasingly digital society, with almost 90% of public services expected to be delivered digitally by 2030. While this digital transformation offers significant opportunities for individuals, businesses and government, it also increases citizens' exposure to cyber risks and highlights a critical gap in the support available to those affected by cyber incidents.

The evidence points to a clear and urgent need for action. Ireland has been identified as one of the most heavily targeted countries for phishing attacks, while globally more than 88.5 million people are estimated to fall victim to cybercrime each year. In Ireland alone, over €300 million was lost to call and text-based scams in 2025, fraudulent payments increased by 26% between 2022 and 2023, and more than 10,000 cyber-enabled crime incidents were reported to An Garda Síochána in 2024. Fraud offences also increased by 73% during the first half of 2025 compared with the same period in 2024. These figures demonstrate that cybercrime is no longer a niche or technical issue; it is a growing societal challenge affecting individuals, families and communities across Ireland.

Cyber incidents now encompass a diverse range of harms and regardless of the nature of the incident, many people share a common experience: they do not know where to turn for trusted advice and support. Existing services provide valuable assistance within their respective remits, but there is currently no single, accessible point of contact to help individuals understand what has happened, identify the most appropriate next steps, and navigate the complex landscape of reporting, technical recovery and victim support.

Ireland therefore requires a dedicated national cyber security helpline that places people at the centre of cyber resilience. The helpline would provide support across the full cyber incident journey, from education and prevention through to compassionate first-line assistance, practical guidance and recovery support. By providing trusted, evidence-based information, helping individuals make informed decisions, and connecting them with the most appropriate services, a national cyber security helpline would strengthen both individual outcomes and Ireland's broader cyber resilience.

The Gap: No one to turn to

While cyber incidents are increasing in frequency and complexity, Ireland lacks a dedicated, accessible service that individuals can turn to for trusted guidance and support. Existing organisations provide valuable assistance within their respective remits; however, many people struggle to identify where to seek help, who to trust, or what steps to take following a cyber incident. As a result, individuals are often left to navigate a fragmented support landscape at a time when they may be distressed, overwhelmed or vulnerable.

Our research highlights the scale of this gap. Across our engagements —

96%

of participants
reported that they did
not know where to
access reliable cyber
safety information

85%

of older adults
described feeling fear
or anxiety when using
digital technologies

36%

said they had no one
to turn to for support
with online concerns

These findings suggest that many people are navigating an increasingly digital world without the knowledge, confidence or support they need to stay safe online.

The emotional impact of this uncertainty was evident throughout our research. Participants frequently described feeling fearful, overwhelmed and lacking confidence when engaging with digital technologies. As one participant explained, "I used to feel safer" (P64), while another reflected, "Fear of the unknown, hackers are getting smarter. Something could happen that I think is okay but it's not" (P1). Others described being "very nervous" (P3), "terrified to be truthful" (P10), or explained that "It moves so fast, hard to keep up" (P8). For many, the fear extended beyond technology itself to a broader sense of vulnerability: "I'd be worried, they're out to catch you" (P19).

Participants also highlighted the absence of accessible support when they encountered digital challenges. One older adult remarked, "No, it's all guesswork

for me. If I ask someone, they laugh and say there's an easier way" (P19), illustrating how uncertainty can be compounded by embarrassment or fear of asking for help. Where support was available, it was typically informal and dependent on family members or trusted organisations, with one participant explaining, "Citizen's Information and family. [I] Ring them or send a message and ask" (P67). Such support, however, is inconsistent and unavailable to many people.

Our findings also demonstrate the continued importance of telephone-based support. Of the initial 146 interviews conducted with older adults, 30 were completed by telephone, reinforcing that many individuals value the opportunity to speak directly with a trusted person rather than relying solely on digital resources. For some participants, particularly those with lower levels of digital engagement, telephone communication was their preferred or only means of accessing information and support.

A small but important group of participants had effectively withdrawn from the digital world altogether. These low-technology users avoided online services, relied almost exclusively on telephone communication, and reported feeling increasingly excluded as essential services continued to move online. Their disengagement was driven by fear of making mistakes, low confidence, and technology-induced stress, demonstrating that the absence of accessible support can contribute not only to cyber vulnerability but also to digital exclusion.

Together, these findings highlight a significant gap in Ireland's cyber resilience. While considerable investment has been made in cyber security awareness, prevention and technical capability, there remains no dedicated service to provide compassionate, human-centred support to individuals when they need it most. A national cyber security helpline would address this gap by providing a trusted first point of contact, helping people understand what has happened, offering clear and consistent guidance, and connecting them with the most appropriate services and supports.

The Cybersafety Project

The Cybersafety project is funded by Research Ireland and throughout the last 3 years has demonstrated that accessible, community-led cyber safety education

can improve confidence, knowledge, and resilience. To date, we have engaged with 45 organisations across 22 counties, built a network of more than 500 stakeholders, and trained 87 Cyber Safety Champions. We support citizens through online resources and have educated 5,620 people through workshops and through the wider ripple effect, directly contributed to protecting many more citizens from cyber harms and potentially preventing millions of cybercrime losses.

Our extensive research has been peer reviewed and published in leading human computer interaction conferences worldwide (Camilleri et al., 2025; Camilleri et al., 2026; Gruben et al., 2025; O'Keeffe et al., 2025; Sheil et al., 2024; Sheil et al., 2025)

We have created a website (www.cybersafety.ie) which hosts blogs and information on local education and numerous resources for all vulnerable populations including people with intellectual disabilities and domestic violence survivors.

Our original plan was a self-directed e-learning course for older adults themselves, but this met with pushback: many told us they would not engage with it alone, as they preferred receiving information from someone they already trusted. We therefore pivoted, designing an e-learning course not for older adults directly but for the people already embedded in their lives — librarians, adult educators, and Education and Training Boards (ETB) and Further Education and Training (FET) practitioners — who are often the first phone call when someone encounters a scam. Alongside this, we deliver free, interactive workshops in community libraries across the country. None of this would have been possible without countless hours spent listening to communities, building trusted partnerships, designing accessible learning, and ensuring that every person we reach feels supported and empowered.

The Need For a Helpline is Evident

Through our extensive interviews and relationship-building with older adults and community groups, a clear theme emerged around what they seek and need: compassionate support and a point of contact that is neither family nor the Gardaí. Lack of support emerged as the greatest challenge for older adults. Many

felt embarrassed to seek help from family, while others found relatives lacked time or patience. Notably, 36% reported having no family support. They expressed a strong need for in-person, over the phone, and online assistance. Participants consistently expressed a desire for accessible, human support and often resorted to asking phone shop staff for assistance. P26 simply wanted "to know what to do," while P48 spoke of the value of "speaking to somebody." Others were explicit about the form this should take: P2 called for a "Helpline," P10 for a "reassurance, phonenumber, genuine and trusted support," and P12 for a "support helpline for queries." This desire for someone reachable in the moment recurred throughout, with P10 describing wanting "somebody at the end of the line," P27 wanting "someone to tell me the risks," and P56 wanting "someone who speaks English, clear information, someone who understands what I'm asking." Calling the Gardaí can feel like a daunting, formal step, and many older adults are intimidated by the idea of reporting something that may turn out to be minor. A helpline offers a calming, grounding first step, giving people a chance to establish whether the situation calls for a password change or genuinely warrants Garda involvement, while also sparing already-stretched Garda resources from queries that don't need them.

As the Cyber Safety project expanded, so did the range of groups we engaged with. We spoke to other vulnerable cohorts, including people with intellectual disabilities, migrants, and domestic violence survivors, each with often very different cyber safety needs. Young adults face distinct challenges of their own, chief among them non-consensual intimate image sharing, a rising and alarming threat to their safety. The psychological toll of image-based sexual abuse (IBSA) is severe and well documented, with growing evidence linking victimisation to suicidal ideation and self-harm. In one of the most widely cited studies, the Cyber Civil Rights Initiative found that 51.7% of non-consensual intimate image victims had attempted suicide (Cyber Civil Rights Initiative, 2014). More recent peer-reviewed research corroborates this pattern: a study of 6,021 individuals found that 43.7% of victims reported depressive symptomatology and 52.1% had engaged in self-harming behaviours (cited in Springer Scoping Review, 2026), while a separate study of cybersexual harassment victims found 22% reported suicidal thoughts within the previous month (cited in Springer Scoping Review, 2026). A 2024 systematic review spanning 21 studies and 32,252 participants concluded that non-consensual image sharing is consistently associated with elevated depression, anxiety, and suicidal ideation among young people (Schmidt et al., 2024). In an Irish context, this harm has played out publicly and with fatal consequences: Dara Quigley died by suicide in 2017 after CCTV

footage of her was shared without consent on social media, at a time when no Irish law criminalized such sharing (Her.ie, 2020). Ireland did not legislate against non-consensual image sharing until the Harassment, Harmful Communications and Related Offences Act 2020, and an ISPCC study found that reported cases disproportionately involve victims aged 18 and 19, who together account for 42% of cases (Oxygen.ie, n.d.). Together, these findings underline the urgent need for accessible, immediate support for victims, of the kind a dedicated helpline is designed to provide. Often these cases are highly sensitive and embarrassing for young adults who are reluctant to share with their parents. Having a helpline to ask what to do in these situations could be lifesaving.

What the Cyber Security Helpline should be

A national cyber security helpline should be designed around the needs of the people it serves. Cyber incidents often leave individuals feeling frightened, embarrassed, overwhelmed, and unsure of what to do next. While technical advice is important, people frequently need reassurance, practical guidance and someone who can help them make sense of what has happened before they can take effective action. Research on cybercrime victims consistently demonstrates that emotional support and trusted guidance are important components of recovery and resilience, alongside technical assistance (Chavan, 2025; Chen et al., 2026).

The service should therefore be compassionate, accessible and human-centred. It should be available to everyone regardless of age, digital literacy or location, recognising that many people, particularly older adults, those living in rural communities, and individuals experiencing isolation, may be more comfortable speaking to a trained adviser over the telephone than navigating online information alone. The helpline should complement existing digital resources by providing a trusted human point of contact when reassurance and personalised guidance are needed.

Central to the service should be the provision of trusted, accurate and consistent information. Individuals affected by cyber incidents are often confronted with conflicting advice from websites, social media, friends and online forums, for example 41% of password advice collected was directly contradicted by another

source (Murray & Malone, 2017). A national helpline would provide evidence-based guidance tailored to each person's circumstances, reducing confusion and enabling individuals to make informed decisions.

The helpline should also provide practical first-line guidance. This includes helping callers understand the immediate actions they should take, preserve digital evidence where appropriate, gather relevant documentation, secure compromised accounts, change passwords, contact financial institutions or online platforms, and understand whether reporting to An Garda Síochána or another organisation is appropriate. Not every cyber incident requires law enforcement involvement, but every individual deserves clear guidance on the options available to them and the likely consequences of each.

Importantly, the helpline should not duplicate the work of existing organisations but rather act as a trusted navigator across Ireland's cyber support ecosystem. Staff would assess each situation and refer individuals to the most appropriate services, including banks, An Garda Síochána, technology platforms, victim support organisations and specialist services where required. In doing so, the helpline would simplify what is currently a fragmented landscape, ensuring that people receive the right support at the right time rather than being left to navigate multiple organisations alone.

By combining compassionate support, trusted information, practical guidance and coordinated referrals, a national cyber security helpline would become a critical component of Ireland's cyber resilience, ensuring that no individual need face a cyber incident without somewhere to turn.

Why Ireland Needs a Cyber Security Helpline Now

Ireland's cyber threat landscape is evolving rapidly. Cyber incidents now extend far beyond traditional computer hacking to include online scams and fraud, phishing, account compromise, digital identity theft, technology-facilitated abuse, social media account takeovers, business email compromise, sextortion, and child sexual abuse material (CSAM)-related concerns. As cyber harms become more diverse and increasingly affect people in their everyday lives, Ireland's support infrastructure must evolve to meet these changing needs.

At present, Ireland has only a partial understanding of the true scale and nature of cybercrime affecting individuals. Many incidents are never reported to An Garda Síochána, financial institutions, or other agencies because victims are unsure whether what they experienced constitutes a crime, do not know where to report it, or believe nothing can be done. As a result, existing statistics are likely to underestimate both the prevalence of cyber incidents and their impact on individuals and communities. This limits Ireland's ability to identify emerging threats, allocate resources effectively, and develop evidence-based public awareness campaigns and policy responses.

A national cyber security helpline would help address this gap. By collecting anonymised, aggregated information on the nature of enquiries it receives, the service would generate valuable insights into emerging scams, patterns of account compromise, technology-facilitated abuse, digital identity threats, and the experiences of vulnerable groups. This evidence could be used to identify trends at an earlier stage, monitor changes in cyber harms over time, and better understand the support needs of the public.

Importantly, the information collected would not simply improve service delivery; it would strengthen Ireland's broader cyber resilience. Anonymised data could inform academic research, public awareness campaigns, national cyber security policy, and the development of targeted interventions for communities most at risk. In this way, the helpline would serve not only as a trusted source of support for individuals but also as a valuable national capability, providing an evidence base to help Ireland anticipate, understand and respond to an increasingly complex cyber threat landscape.

Methodology

This position paper draws upon research and public engagement undertaken by the Cyber Safety for Vulnerable Populations team over the past three years. The findings are informed by real engagements with members of the public seeking cyber safety advice and support, together with qualitative research approved by the Munster Technological University Research Ethics Committee (Ethical Approval No: MTU-HREC-FER-25-008-A). Participant quotations have been anonymized to protect privacy. The Cyber Safety Project is funded by the EU Commission

Conclusion

Ireland has invested significantly in cyber security capability, awareness and incident response. However, a critical gap remains for individuals seeking help after experiencing a cyber incident. A national cyber security helpline would provide compassionate support, trusted guidance and coordinated referrals, while simultaneously improving understanding of cyber harms across Ireland. As cyber incidents continue to affect people of all ages and backgrounds, ensuring that everyone has somewhere to turn should become a core component of Ireland's cyber resilience.

References

1. Chavan, Girish. (2025). Loss of Trust: How Cybercrime Changes the Way Victims See the Internet. *International Journal of Applied Sciences and Radiation Research*. 2. 10.22399/ijasrar.45.
2. Chen, X., Tran, M., Deng, Y., Acharya, B., and Zou, Y. 2026. From Harm to Healing: Understanding Individual Resilience after Cybercrimes. In Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26). Association for Computing Machinery, New York, NY, USA, Article 1315, 1–22. <https://doi.org/10.1145/3772318.3791486>

3. Cyber Civil Rights Initiative. (2014). Effects of Revenge Porn survey data, cited in PrivacyRadar, "25 Revenge Porn Statistics and Surprising Facts." <https://privacyradar.com/statistics/revenge-porn-statistics/>
4. Schmidt, F., Varese, F., Larkin, A., & Bucci, S. (2024). The Mental Health and Social Implications of Nonconsensual Sharing of Intimate Images on Youth: A Systematic Review. *Trauma, Violence, & Abuse*. <https://journals.sagepub.com/doi/10.1177/15248380231207896>
5. Mental Health on Victims of Non-consensual Intimate Image-sharing: A Scoping Review. (2026). *Sexuality Research and Social Policy*. <https://link.springer.com/article/10.1007/s13178-026-01312-x>
6. Her.ie. (2020). Ireland's image-based sexual violence laws. <https://www.her.ie/news/irelands-image-based-sexual-violence-laws-revenge-porn-513656>
7. Oxygen.ie. "I was 12": The Reality of Image Based Sexual Abuse in Ireland. <https://www.oxygen.ie/i-was-12-the-reality-of-image-based-sexual-abuse-in-ireland/>
8. Sheil, A., Camilleri, J., Cronin, M., Gruben, M., O'Keeffe, M., Murray, H., & Das, S. (2024). Enhancing Personalised Cybersecurity Guidance for Older Adults in Ireland. In Companion Publication of the 2024 Conference on Computer-Supported Cooperative Work and Social Computing (CSCW Companion '24), November 9-13, 2024, San Jose, Costa Rica. ACM, New York, NY, USA (pp. 478-484). <https://doi.org/10.1145/3678884.3681894>
9. Sheil, A., Camilleri, J., O'Keeffe, M., Gruben, M., Cronin, M., & Murray, H. (2025). "I'm 73, you can't expect me to have multiple passwords": Password management concerns and solutions of Irish older adults. Symposium on Usable Security and Privacy (USEC) 2025, San Diego, CA, United States. <https://dx.doi.org/10.14722/usec.2025.23017>
10. Gruben, M., Sheil, A., Das, S., O'Keeffe, M., Camilleri, J., Cronin, M., & Murray, H. (2025). "It's Like Not Being Able to Read and Write": Narrowing the Digital Divide for Older Adults and Leveraging the Role of Digital Educators in Ireland. In Proceedings of the Nineteenth International Conference on Tangible, Embedded, and Embodied Interaction (TEI '25), March 04-07, 2025, Bordeaux/Talence, France. ACM, New York, NY, USA (pp. 1-15). <https://doi.org/10.1145/3689050.3704945>
11. Camilleri, J., Sheil, A., O'Keeffe, M., Cronin, M., Gruben, M., & Murray, H. (2025). Cybersafety Card Game: Empowering Digital Educators to Teach Cybersafety to Older Adults. In Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA '25), April 26-May 1, 2025, Yokohama, Japan. ACM, New York, NY, USA (12 pages). <https://doi.org/10.1145/3706599.3719806>
12. O'Keeffe, M., Camilleri, J., Sheil, A., Das, S., Gruben, M., Cronin, M., Curtin, M., Long, A., & Murray, H. (2025). Cybersecurity Concerns of Older Irish Adults: A Comparison

Across High, Medium and Low Tech Usage. In 2025 European Symposium on Usable Security (EuroUSEC) (pp. 138-150). IEEE. 10.1109/EuroUSEC69254.2025.00023

13. Camilleri, J., Sheil, A., Cronin, M., Gruben, M., Calnan, E., Duffy, A.R., Murray, H., & O'Keeffe, M. (2026). "Your Voice is Lost": How Migrant Community Workers Navigate Digital Safety Challenges in Ireland. In Extended Abstracts of the 2026 CHI Conference on Human Factors in Computing Systems (CHI EA '26), April 13–17, 2026, Barcelona, Spain. ACM, New York, NY, USA, 9 pages. <https://doi.org/10.1145/3772363.3799380>
14. Murray, H., & Malone, D. (2017). Evaluating password advice. In 2017 28th Irish Signals and Systems Conference (ISSC) (pp. 1–6). IEEE. <https://doi.org/10.1109/ISSC.2017.7983609>

Cyber Safety for Vulnerable Populations · Munster Technological University · Funded by
Research Ireland