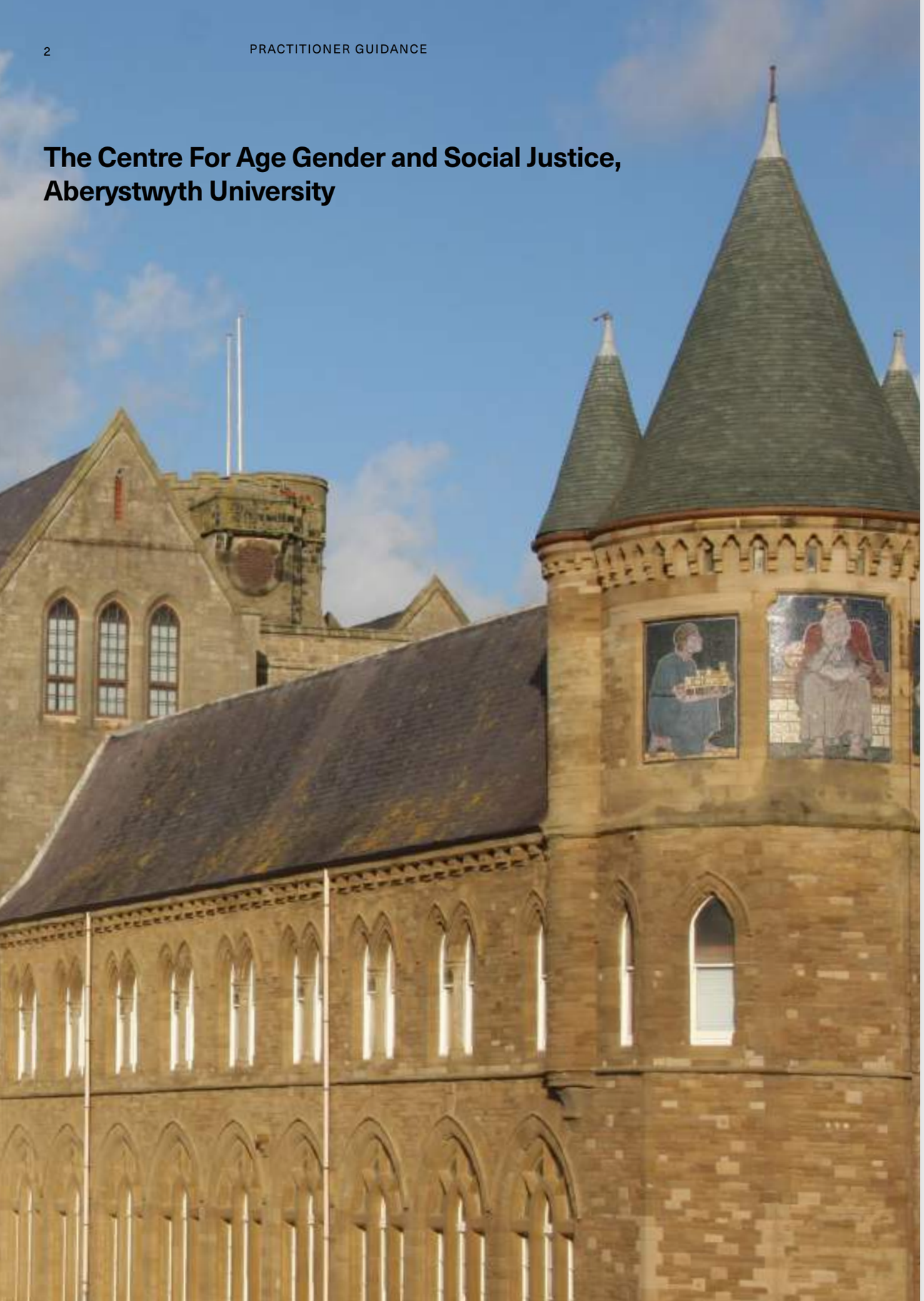
PRACTITIONER GUIDANCE

Supporting Older Victims of Technology-Facilitated Domestic Abuse

Written by Allan Rush, Joshua Roberts, Rebecca Zerk, Elize Freeman and Michelle John



The Centre For Age Gender and Social Justice, Aberystwyth University

Dewis Choice
Centre for Age Gender and Social Justice
Aberystwyth University
Penglais
Aberystwyth
Ceredigion
SY23 3FL

Contact

choice@aber.ac.uk

Authors

Allan Rush, Joshua Roberts, Rebecca Zerk,
Elize Freeman and Michelle John

Acknowledgements

The production of the guidance was funded by the National Lottery Community Fund. We are grateful for the support provided by our funders in our commitment to promoting the needs, rights and entitlements of older victim-survivors of domestic abuse.

CRONFA GYMUNEDOL COMMUNITY FUND

Contents

Introduction

The digital age has reshaped how individuals communicate, manage finances, and access essential services, offering greater convenience and efficiency. While technology has the potential to reduce social isolation and enhance access to support, its rapid evolution has also created new barriers for some groups of people. Limited digital access has been linked to economic disadvantage and disproportionately affects older adults, people with disabilities, and those in rural areas with inadequate internet infrastructure (Good Things Foundation, 2024).

In 2019, around four million UK residents had never accessed the internet, with 94% of them aged 55 years and older (Tabassum, 2020). Digital engagement among older adults increased significantly during the COVID-19 pandemic, however, those aged 55 and over remain the demographic most likely to have never used the internet (Tabassum, 2020). Although the gender gap in relation to older peoples' internet use decreased during the pandemic, older women, aged 65 years and over, are still less likely to use the internet than older men (Bünning et al. 2023).

A key driver of increased internet use by older people is necessity, as more essential services move online, such as healthcare (Dewis Choice, pending). For instance, older adults were identified as the most active users of the NHS application (app) (NHS England, 2023). Additionally, the rates of older people using digital communication to maintain social connections with friends and family have increased, particularly through email.

Despite the rise in internet use for specific activities, older adults still remain less engaged with online financial services compared to younger age groups. Those aged 55 years and over are the least likely to use internet banking, with security concerns being a primary barrier (Smith, 2020). A report by Santander (2020) found that many older adults still prefer in-branch banking due to fears of exposure to online fraud. Similarly, a study by Vodafone (2022) revealed that individuals aged 65 years and older were less likely to use online shopping services compared to younger age groups, citing concerns about digital security and scams.

Limited exposure to technology, lower confidence in navigating digital tools, and unfamiliarity with online risks can expose older adults to risks such as scams, fraud, and technology-facilitated

abuse (Independent Age, 2024). A report by Lloyds Bank (2024) found that among individuals identified as having very low digital literacy, almost 90% were over the age of 50 years. Limited access to technology can lead to reliance on others to access digital services on older peoples' behalf, which can limit their ability to control their data security (Hasse et al., 2021).

As more services shift online, increasing numbers of older people rely on family members or caregivers to manage digital tasks on their behalf (Age UK, 2023; Carers UK, 2023; Hasse et al., 2021). Without direct control over their online accounts, older adults can be at heightened risk of exploitation by the people closest to them. This dependency can leave older people at increased risk of financial abuse, fraud, identify theft, and coercion.

A Practitioner-Focused Approach

Addressing the Gap: Ageing Population and Technology-Facilitated Abuse

Frontline staff and practitioners and the criminal justice system are increasingly aware of the role of technology in facilitating domestic abuse. However, the nature and impact of technology-facilitated abuse on older victims remains underexplored.

This guide aims to address this gap and brings together knowledge, insights, and data from:

Dyfed-Powys Police safeguard people living in, working in and visiting the counties of Carmarthenshire, Ceredigion, Pembrokeshire and Powys which equates to the largest geographical policing area in England and Wales. This includes over one million hectares of agricultural land, more than 350 miles of coastline, and stretches from St David's in the west to Crickhowell in the east, and up to Welshpool and Machynlleth in the north.

Dyfed-Powys Police serve more than 515,000 people, which rises significantly with tourists each year. Almost half of the total resident population is aged 45 and over, and 22% are aged over 65.

Based at Aberystwyth University's Centre for Age, Gender and Social Justice, the Dewis Choice Initiative has co-produced a pioneering grassroots intervention, developed with the community to support older victim-survivors of domestic abuse by partners, ex-partners, or adult family members. Combining direct service delivery with ground-breaking research, Dewis Choice leads the first prospective longitudinal study exploring decision-making in later life. By listening to older victim-survivors, the Initiative identifies what works and how services, including housing, policing, health, social care, and the third sector, can improve their responses. This rights-based, research-informed model ensures support is tailored to the specific needs of older adults.

Based in Shropshire and Derbyshire, PEGS (Parental Education Growth Support) is a pioneering lived-experience social enterprise working alongside parents, carers and guardians impacted by child-to-parent abuse (CPA), including abuse from adult children. Combining direct service delivery, advocacy, professional training, and policy influence, PEGS is driving forward national understanding of CPA and improving frontline responses.

Through ongoing engagement with thousands of parents, PEGS co-produces and delivers services that reflect real-world experiences, while informing best practice across policing, education, housing, health, social care and the third sector.

This rights-based, trauma-informed model ensures that support is tailored to the needs of parents, and that professionals are equipped with the tools and understanding to respond effectively. PEGS also contributes to national policy, having helped secure the inclusion of CPA in the Domestic Abuse Act 2021 statutory guidance, and has spearheaded the UK's annual Child to Parent Abuse Awareness Day.

This guide serves as a comprehensive toolkit for practitioners responding to technology-facilitated abuse, providing actionable advice and guidance to frontline staff and practitioners working with older victims of domestic abuse, stalking and harassment.

Important Note: This guidance is intended for use by professionals only. The document should **not** be shared directly with victims, due to the potential risk of it being accessed by the perpetrator.

Theguidance aims to help practitioners to:

1. Understand how technology can be misused to perpetrate abuse against older victims.
2. Recognise how coercive control is linked to technology-facilitated abuse in cases of intimate partner abuse and adult family abuse involving older adults.
3. Access practical advice and guidance to support older victims in enhancing their cyber security.
4. Integrate protective strategies into ongoing safety planning and risk management with older victims.
5. Develop an understanding of key legislation relevant to technology-facilitated abuse.

The guide will cover a wide range of technology that can be misused by perpetrators, although it is not an exhaustive list.

Please note, while this guidance contains up-to-date technical advice, it does not make any attempt to assess the risk of applying this advice. Practitioners should consider the individual circumstances of each older adult they are engaging with and to decide how and when the advice presented should be adopted to safeguard the victim. For example, where a perpetrator and victim are living together, behaviours that can be detected by a perpetrator, such as changing a password to lock a perpetrator out of an account, may place a victim at increased risk of harm. A decision may be made to delay the action until the victim is no longer living with the perpetrator.

For the purposes of this guide, the terms 'older adults' and 'older people' refers to adults aged 55 years and above to reflect the available research and literature. The guide includes case studies that have been anonymised. We will use the term 'victim' throughout the guide to reflect Crown Prosecution Service (CPS) legal guidance. The term 'victim' encompasses other terms such as 'complainant(s)' and 'survivor(s)'. When responding to older adults who are experiencing, or who have experienced, domestic abuse, stalking or harassment, practitioners should use terminology that the older adult is comfortable with.

Understanding Domestic Abuse and Technology-Facilitated Harm

Domestic abuse is legally defined in Section 1 of the Domestic Abuse Act 2021 (England and Wales) as:

> *"a single incident or course of conduct between those who are aged 16 years or over who are, or have been, intimate partners or family members."*

This definition is gender-neutral, acknowledging that women, men, and non-binary people can be victims.

The legal definition encompasses various forms of abuse, including:

- Physical abuse
- Sexual abuse
- Economic abuse
- Emotional and psychological abuse
- Coercive or controlling behaviour

Dewis Choice (2015-2025) research has found that like younger age groups, for many older victim-survivors, domestic abuse is more than a single incident and involves ongoing patterns of harmful behaviours, often involving multiple forms of abuse (Wydall et al., 2021). Perpetrators may target more than one individual within an intimate relationship or family unit. Additionally, older victim-survivors may be subjected to abuse from multiple perpetrators either simultaneously or co-currently.

Coercive or Controlling Behaviour

Recognising the multifaceted nature of domestic abuse—extending beyond physical violence—the UK Government criminalised coercive and controlling behaviour under section 76 of the Serious Crime Act 2015.

For the crime of coercive or controlling behaviour to have taken place, Section 76 of the Serious Crime Act states that: The coercive behaviour must take place "*repeatedly or continuously"*. Continuously means on an ongoing basis.

The pattern of behaviour has to have a *"serious effect"* on the victim - this means that they have been caused to

EITHER
- fear that violence will be used against them on *"at least two occasions"*,

OR
- they have been caused serious alarm or distress which has a "substantial adverse effect" on the victim's usual day-to-day activities.

The behaviour must be such that the perpetrator *"knows"* or *"ought to know"* that it will have a serious effect on the victim.

- The perpetrator and victim are, or have been in an intimate relationship

OR
- The perpetrator and victim are relatives (as defined by the Family Law Act 1996)

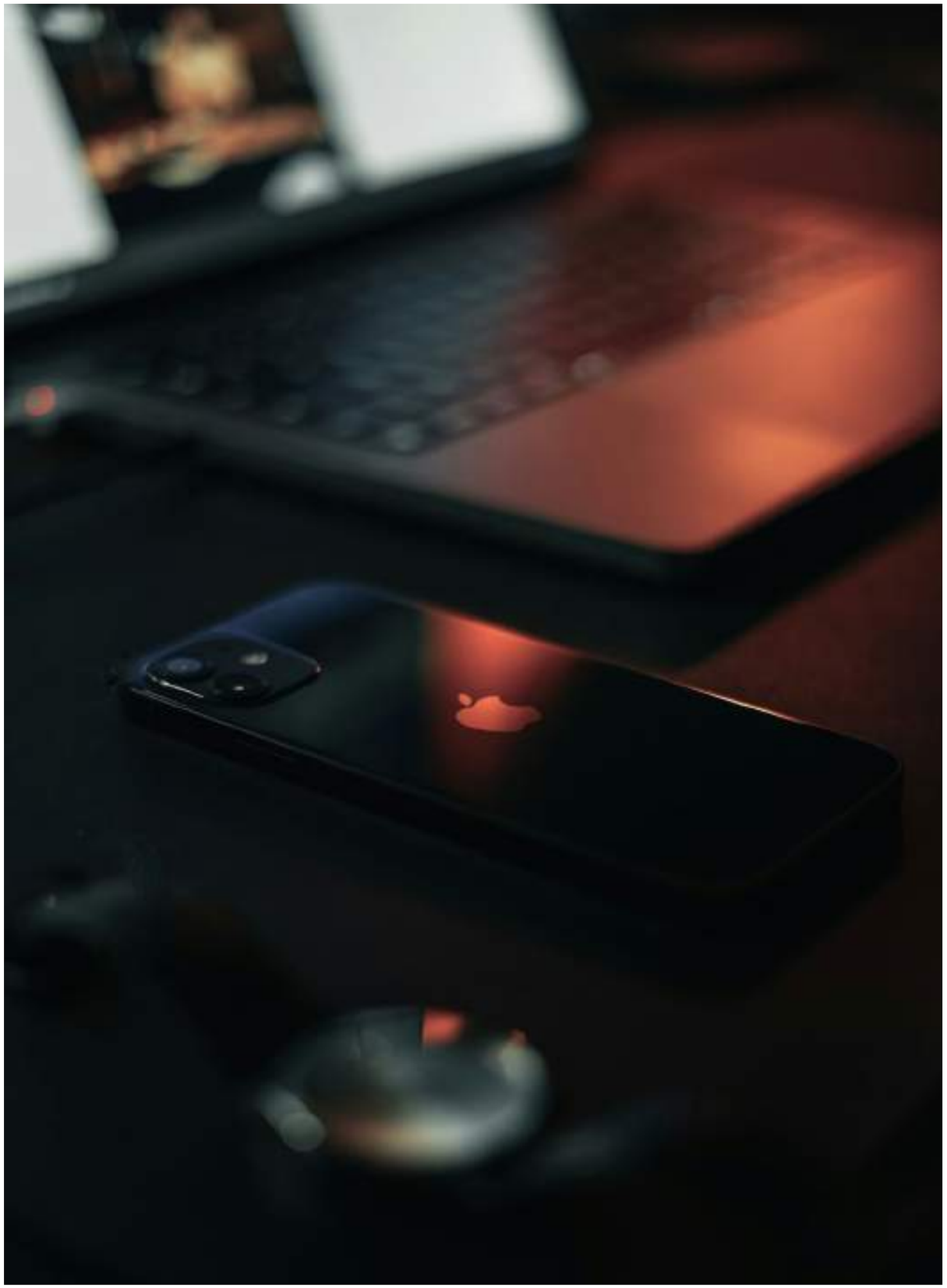
The legislation firmly establishes coercive or controlling behaviour as a criminal offence (see Bishop and Bettinson, 2018) and is regarded as a 'landmark step' in better reflecting people's experiences of victimisation (Women's Aid, 2023).

Coercive control, as described by Stark (2007), is a pattern of abusive behaviours used by one person to manipulate, dominate and exploit another. Controlling tactics can include threats, constant surveillance, excessive monitoring (Okun, 1986) and isolating the victim from friends and family. By asserting power and control, the perpetrator erodes the victim's independence, forcing the victim to conform to specific behaviours and thought patterns through intimidation, pressure, or threats. Such controlling conduct can infiltrate every facet of the victim's life.

Unlike overt forms of abuse, coercive or controlling behaviours can be subtle, making it difficult for victims and even practitioners to identify. Whilst there is a large body of research that discusses coercive or controlling behaviours, the research is primarily focused on the experiences of younger, heterosexual, female victims who have been subjected to abuse by male partners within intimate relationships (Freeman, 2022).

For older adults, coercive or controlling behaviour may present differently to younger adults (Dewis Choice Adapted Power and Control Wheel: Appendix A.). Controlling behaviours may be masked by traditional gendered roles (Zerk, 2025). For older people with care and support needs, coercive or controlling behaviours may be guised as 'caregiving' which may make it more difficult for the older adult to identify the behaviour as abusive (Older People's Commissioner for Wales, 2017). Perpetrators may take advantage of their relationship with the older person, as well as expectations of trust, or lack of legal or financial knowledge, to exert control over their decisions and financial resources.

With the rise of digital technology, coercive or controlling behaviours are increasingly being carried out using digital devices and online, further extending perpetrators' reach and influence.



Nature and Extent of Technology-Facilitated Abuse

Technology-facilitated domestic abuse, sometimes referred to as digital abuse, primarily involves the use of digital technologies and tools to monitor or control victims, or to carry out financial abuse. Abuse via technology is not a new phenomenon and is likely to occur alongside other forms of abuse (Brookfield et al., 2024; Cuomo and Dolci, 2021; Kelly, 1988). However, unlike other forms of abuse, technology-facilitated abuse does not require physical proximity to the victim. Perpetrators can misuse technology to monitor victims' activities in real time or retrospectively, often without the victims knowledge (Harris and Woodlock, 2018; Leitao, 2021).

Although technology-facilitated abuse is recognised as a form of domestic abuse, there is currently no statutory or widely accepted definition in England and Wales.

The Rise of Technology-Facilitated Domestic Abuse

Perpetrators are increasingly using digital technology to threaten, stalk, or harass victims (Christie and Wright, 2020). An understanding of when abuse may occur is also important, as although technology-facilitated abuse can happen during a relationship, 80% of reports are initiated after the breakup of a relationship (Action Fraud, 2020-2023).

According to a survey by Refuge (2021):

> *Between April 2020 and May 2021, there was a 97% increase in complex cases involving technology-facilitated abuse that required specialist input.*
> *It is estimated that 1 in 3 women have experienced online abuse perpetrated on social media or other online platforms at some point in their lives;*
> *of these women 1 in 6 have experienced this abuse from a partner or ex-partner.*

Despite these alarming figures, there is limited data on the experiences of victims who are subjected to technology-facilitated abuse perpetrated by adult family members, or how this form of abuse effects older people.

Dyfed-Powys Police Crime Data – Older Victims

Between 1st May 2024 and 30th April 2025 (12-month period), Dyfed Powys Police recorded 951 domestic related crimes involving victims aged 55 and over. A review of the case summary data for these crimes identified 101 technology employed offences. However, the actual number of domestic related crimes involving technology is likely higher, as its use is not routinely captured in case summaries unless it is identified as a primary factor.

The identified offences involving technology were grouped across 23 Home Office categories and are broken down as follows:

Technology Employed	Number of Offences	% of Total Domestic Related Offences (n=951)
AirTag (Small tracking device/tab)	1	0.1%
Bank Account Access	14	1.5%
Digital Communications (calls, texts, voicemails, social media messages/posts, emails)	82	8.6%
Drone	1	0.1%
Mobile Telephone Tracking & Recording	1	0.1%
CCTV	1	0.1%
Video	1	0.1%
TOTAL	**101**	**10.6%**

Dyfed-Powys Police crime data, highlights that digital communications are by far the most commonly used form of technology in domestic related technology employed crimes involving older victims.

PEGS – Older Victims of Digital Abuse

PEGS (Parental Education Growth Support) includes a specific question on its referral form that asks individuals about experiences of digital abuse. This encompasses technology-facilitated monitoring, stalking, harassment, and controlling behaviour. A review of referral data from PEGS involving 350 older individuals, aged 56 and over, revealed that 14% (n=49) reported experiencing digital abuse. In these cases, the abuse was perpetrated by either their child or someone for whom they had parental responsibility, such as a grandchild.

Older Adults Experiences of Technology-Facilitated Abuse

For older individuals, technology-facilitated abuse can be particularly insidious due to their often-limited familiarity with technology, making them less likely to be aware of, or recognise abusive behaviours. In addition, older individuals may be more dependent on perpetrators for technological support or navigation. In this context, technology becomes a weapon for perpetrators to maintain dominance, isolate victims, and manipulate their sense of safety and autonomy to financially exploit.

This section of the guide will explore seven forms of technology-facilitated abuse including: tracking and surveillance; monitoring; control and manipulation of smart devices; misuse of digital payment platforms and subscriptions; unauthorised use of online banking and shopping accounts; coercive control under the guide of help; and image-based abuse.

Tracking and Surveillance

Digital technologies have significantly increased access to personal information, including exact locations, social networks, and daily routines. In the context of domestic abuse, perpetrators may exploit these technologies to track or surveil their intimate partner or family member. Tracking refers to following a person's movements or actions, often using GPS technology, location-sharing apps, or even monitoring transport and spending patterns.

Tracking:

Perpetrator Behaviour

- *Smartphones, Sat Navs and GPS:* Perpetrators may install tracking apps or utilise built-in GPS features on smart mobile devices to monitor the victim's location. Older adults, who may not be aware of these features (or how to disable them), are particularly vulnerable in this scenario.

- *Bluetooth Trackers:* Specialist devices that can be purchased and hidden in the vehicle. These may be powered by the car (and stop transmitting when the engine is off) but can also be battery powered.

- *Dashcams:* Are used to record what happens during a vehicle's journey. However, they can be misused as a tracker to see where the vehicle has been. Some dashcams also record inside the vehicle as well as outside. Some dashcams use cloud storage and can livestream footage.

- *Wearable Devices:* Fitness trackers or smartwatches with location-sharing capabilities may be exploited to track victims' whereabouts.

- *Social Media:* Location tracking through social media 'check-ins' or online activity.

- *Location Sharing via an Account*: If using an app or service that can be logged in elsewhere, someone else could track your location by logging into the account. For example, when using Google Maps while logged into a Google account, if someone else can log into your Google account on a different device they will be able to see where other account users are.

- *Dementia Trackers:* Though a useful device for safeguarding individuals with dementia, they can be misused as a tool to control and limit an individual's autonomy.

- *Shopping apps/Accounts*: Online shopping accounts can hold sensitive information, including bank details, home address, and purchasing history. A perpetrator who still holds access to these accounts may use such information to stalk and harass a victim.

Practitioner Quick Action Response

Educate Victims on Device Settings and Features:

- If a perpetrator and a victim have access to the same car, then the victim may want to remove the history of visited destinations that will be stored within the car's built-in satnav. Check the car's manual (or manufacturer's website) for details of how to do this. If the victim uses a separate mapping tool (for example Google Maps), then a perpetrator with access to their Google account will also be able to view a list of recent places. When deleting sensitive locations from the satnav or vehicle history, victims should do so where they won't be seen by the perpetrator - before setting out for home, or somewhere along the way (safely parked).

- If a victim suspects that they are being stalked through a tracker on their car, they should report this to the police, who have specialist equipment to check over vehicles. Victims may also want to speak to their car dealerships or a mechanic about 'sweeping' the car for tracking devices that a perpetrator may have attached to the car to monitor it remotely.

- If the victim is able to, they should control access to the dashcam, any cloud storage, and any device on which footage is held, using a strong, separate password.

- If a victim is driving to a sensitive location - e.g., a police station, health services, refuge, etc. - they could set the satnav to a nearby location rather than the exact place. The perpetrator then cannot see their exact destination in either satnav history or vehicle tracking. They may want to support their 'alibi', e.g. buying something from shops if that is where they claim to have been.

- Explain how location-sharing features work on smartphones, wearable devices, and apps. Demonstrate how to disable GPS or location tracking settings on commonly used devices.

- Encourage the removal of any unfamiliar or suspicious apps and recommend installing trusted security software to detect spyware.

- Keep the paired wearable device away from the perpetrator and change passwords on the paired device, and online account if applicable.

- If the older person wants to share location, for example, Life360 or Snapmap in Snapchat, ask them to consider who they want to share with and whether this needs to be always shared. Encourage them to think about the reason they are sharing their location, and keep them to a few, trusted individuals.

- If the older adult does not need location tracking in an app, turn it off. This can be done via the phone's settings by turning off location services for the app. In some apps it can also be done in the app as well - e.g. for Snapchat you can both turn off location services in settings, and you can set 'ghost mode' for Snapmap (meaning no one can see your location).

While tracking may involve occasional or specific checks, surveillance tends to be more sustained and intrusive. Surveillance involves continuous or systematic monitoring, typically carried out without the victim's awareness. This could include covertly accessing phone records, monitoring social media interactions, or using spyware to observe online activity.

Surveillance:

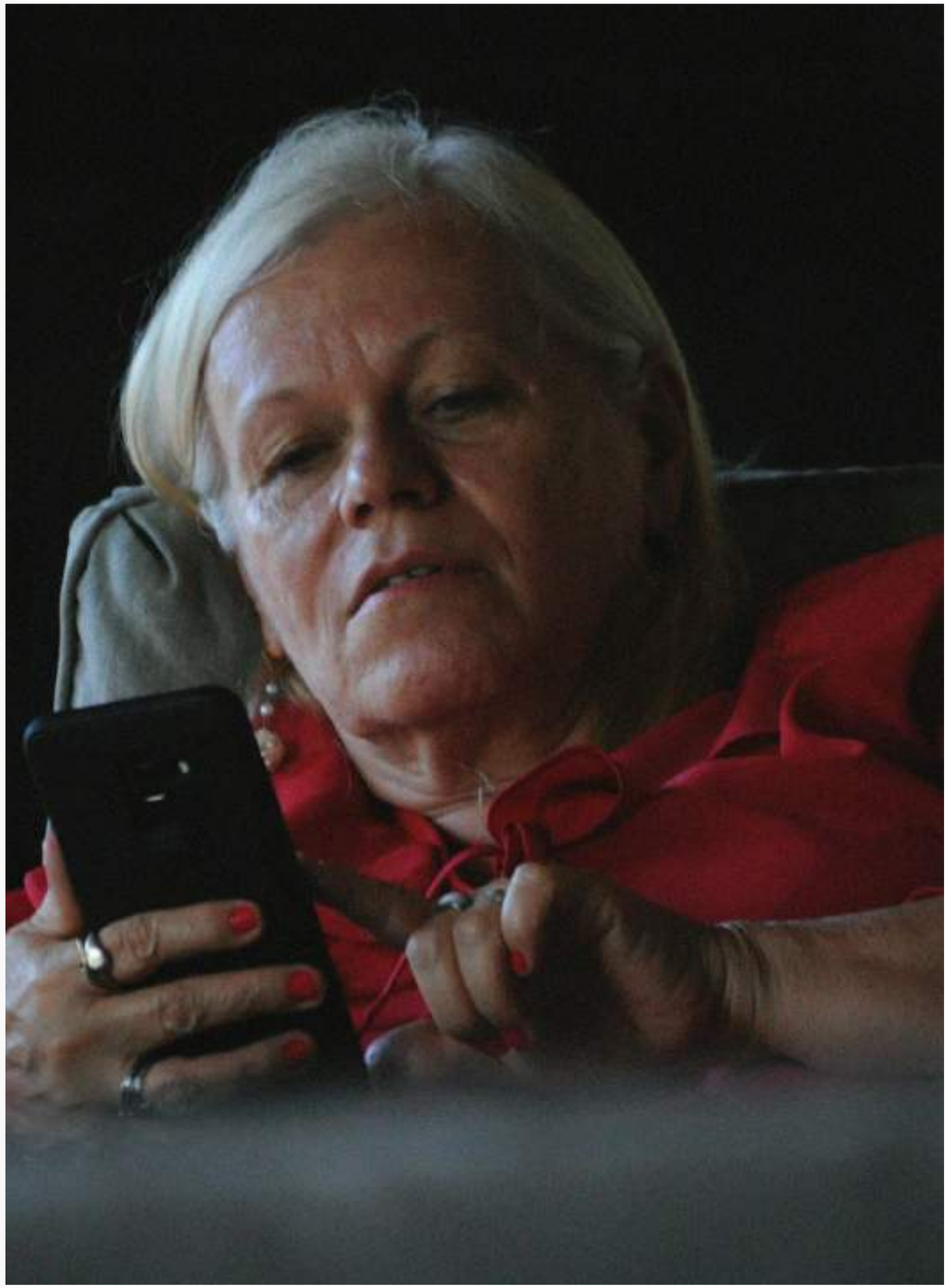
Perpetrator behaviour (without the victims' knowledge)

- Smart Home Devices: Internet-connected devices such as cameras, doorbells, voice activated speakers, or monitors (use of baby or grandparent monitors) could be accessed remotely by perpetrators to observe the victim's daily activities without their knowledge.
- Secretly recording victim with cameras e.g. CCTV
- Spyware or stalkerware installed on a device to track the victim without their knowledge. This software can be bought online and installed easily if the perpetrator can access the device. Examples of this software include FlexiSpy and WebWatcher.
- Some spywares can include a SIM card which can be used as a listening device within a vehicle.

Practitioner Quick Action Response

Advise victims how to secure Smart Home Devices by:

- Resetting login credentials for smart home devices (e.g., doorbells, cameras, voice-activated speakers or baby monitors).
- Using unique, strong passwords and enabling "two-step verification" to prevent remote access by the perpetrator.
- Disconnecting devices from shared accounts that the perpetrator might control.
- Identifying and removing apps on a device that the older person has not installed.
- Factory resetting devices where it is suspected a perpetrator has installed spy/stalkerware. If the perpetrator has, or has had access to the device, change any passwords or codes they may know, and remove their biometric details if these have been used.



Case in Practice: Surveillance through Hacking and Unauthorised Access

Jenny, aged 62 years

Jenny's partner, Paul, became increasingly controlling and physically abusive over their ten-year relationship. Following repeated police callouts to their home, Paul moved into a nearby property. However, despite their separation, Jenny continued to experience abuse in the form of stalking and harassment.

Jenny noticed that Paul always seemed to know her movements in advance, including when she was expecting visitors or tradespeople. She described feeling as though she was under constant surveillance but was unsure how Paul was accessing this information.

How Technology Was Misused:

- Paul had gained unauthorised access to Jenny's email account, allowing him to monitor her private correspondence.
- He used this access to read messages between Jenny and her family, friends, and service providers.
- Paul created a second email account using Jenny's details, impersonating her to communicate with others without her knowledge.

Intervention and Support:
Jenny was supported to:

- Cancel her compromised email account and set up a new, secure one.
- Identify all the digital platforms and devices linked to her old email and update them with the new credentials.
- Strengthen her digital security by setting strong passwords and enabling two-step verification.

Jenny's case highlights how perpetrators can exploit technology to continue exerting control post-separation. It also highlights good practice response to ensuring digital safety measures are put in place to help safeguard the older adult from further abuse.

Both tracking and surveillance can be powerful tools used in coercive control, enabling perpetrators to restrict a victim's freedom, instil fear, and exert dominance without needing to be physically present.

Monitoring

Perpetrators of domestic abuse can misuse technology as a tool for oversight and control, closely monitoring a victim's movements, activities, and interactions with others (Tanczer et al., 2018, 2021; Lopez-Neira et al., 2019). This form of abuse enables perpetrators to enforce victim's compliance with their rules, restrict access to support networks, and limit autonomy. Through spyware, location tracking, or monitoring phone and social media activity, perpetrators can exert constant oversight, where victims are watched and controlled at all times. In some cases, they may also restrict or hinder access to communication, blocking contact with friends, family, or support services. This technological control reinforces the victim's isolation and dependency on the perpetrator, making it even more difficult for the victim to seek help or escape the abusive situation.

Perpetrator Behaviour

- Overtly monitoring day-to-day communication and activities, including phone call logs, texts and social media and messaging services, and internet history.
- Utilising shared and remote access, users can listen into and record conversations.
- Access live video streams of household movements.
- Spyware or stalkerware may be installed onto a phone or other device to obtain passwords covertly.
- Spyware can be misused to monitor device activity, blocking functions, deleting data and accessing the camera or microphone (Yardley, 2020).
- If the victim has a joint bank account with the perpetrator or the perpetrator has the log in details of the victim's bank account, they will be able to see the details of any payments the victim has made, including locations.
- Perpetrators can monitor financial transactions to control spending; this may include setting up alerts to notify of any purchases or spending patterns.
- Video calls can be monitored by perpetrators to see where the victim is and who they are with.
- Digital payment platforms, such as PayPal, can be misused by perpetrators who have access to transfer funds without the victim's knowledge, as well as monitor and track the accounts activity and transactions.

Practitioner Quick Action Response

- If accepting a video call, the older adult should ensure no items in the background indicate their location (e.g. view from window, addressed paperwork). To prevent tracking (approximate) location via the victim's IP address, the NCSC (National Cyber Security Centre) recommends using 3/4/5G instead of Wi-Fi.
- Where safe to do so, the victim should be advised to open a separate bank account in their name only that only they have access to.
- Most banks give the option of using two-step verification/Multi-factor authentication (2SV/2FA) when using online banking. Turning this on will ensure a perpetrator can't access the account even if they know/guess the password/PIN. This will add extra security when a victim logs in to their online account. It confirms a login is genuine through a second device, typically a code that is sent to a mobile phone via SMS text message.

Case in Practice: Technology-Assisted Monitoring and Harassment

Pete, Aged 64 years

Post-Separation Economic Abuse and Harassment

Pete had been experiencing emotional, economic, physical abuse, and coercive control from his female partner for over six years. After a violent assault, Pete was hospitalised for treatment.

While in hospital, Pete asked his son to check his phone for messages. His son discovered that Pete's partner had been deleting messages and blocking friends and family from his phone. Pete explained that his partner knew his phone password and had been regularly accessing his device multiple times a day.

Pete provided a statement to the police about the physical assault, and his partner was arrested. However, he did not disclose to the police that his partner had accessed his phone and controlled his digital communication, nor were these questions asked by the police.

How Technology Was Misused:

- Pete's partner repeatedly accessed his phone without consent, deleting messages and blocking contacts to isolate him from his support network.
- After separation, his ex-partner continued to harass him, using phone calls, text messages, and direct messaging throughout the day and night.
- His ex-partner also contacted Pete's daughter persistently, forcing her to disconnect her landline due to the volume of calls.

Intervention and Support:
Pete was supported to:

- Temporarily move in with his daughter following the separation.
- Secure his phone and online accounts by changing passwords, enabling two-factor authentication, and restricting account recovery options.
- Report ongoing harassment to the police, helping him consider obtaining a non-molestation order to prevent further contact.

Reflections on Pete's Experience:

Pete's case highlights the intersection of coercive control and digital harassment. Practitioners must be aware that post-separation abuse can persist digitally, making continued support and safety planning essential.

Key Considerations for Practitioners:

- Perpetrators may use digital tools to isolate victims by blocking or deleting messages, making it harder for them to reach out for help.
- Technology-facilitated harassment often escalates post-separation, requiring legal interventions such as non-molestation or stalking protection orders.
- Legal and digital safeguarding measures are crucial, including restraining online communication and implementing robust digital security.

Control and Manipulation of Smart Devices

Smart home devices are internet-connected appliances and systems that enable the remote control, automation, and monitoring of various household functions. These devices can be accessed and controlled remotely from anywhere with an internet connection, allowing individuals to operate them regardless of their physical proximity to the household they are kept. While offering increased convenience and efficiency, these devices can be susceptible to manipulation by a motivated perpetrator if not secured effectively.

Perpetrator Behaviour

- *Smart Thermostats:* Using home automation to control heating remotely to leave victims either too hot or too cold.
- *Smart Lighting Systems:* These systems use home automation to control lights remotely, leaving on or turning off lights. This behaviour may be used to create fear or distress.
- *Smart Locks:* Perpetrators can remotely control digital locks to deny access to or trap victims inside their homes.
- *Digital Assistants (e.g., Alexa, Google Home):* These devices can be used to issue commands, gather information, or create an atmosphere of intrusion and control.

Practitioner Quick Action Response

- *Identify Unauthorised Control:* Help victims recognise signs of unauthorised control, such as sudden changes in temperature, lighting, or locked doors that they did not initiate upon command. Use device settings to check for linked accounts or remote access permissions.
- *Reset Devices to Factory Settings*: If the victim agrees, reset devices like thermostats, locks, or digital assistants to factory settings to remove any access the perpetrator may have. Reconfigure the devices with secure credentials.
- *Provide Support Resources:* Refer victims to local services or online resources that specialise in technology abuse. The National Cyber Security Centre (NCSC) or similar organisations may offer additional tools to secure devices.
- *Emergency Safety Planning:* Work with victims to create a safety plan in case smart devices are used to trap them or escalate abusive behaviour. This might include having a spare key for smart locks or access to a trusted neighbour's phone for emergency communication.

Misuse of Digital Payment Platforms and Subscriptions

Digital payment platforms are online services that facilitate the electronic transfer of funds between individuals and businesses. These platforms enable users to make, receive, and manage payments securely via the internet, often utilising methods such as credit or debit cards, bank transfers, and digital wallets. The platforms typically incorporate features like fraud detection, currency conversion, and robust security measures to ensure safe and efficient transactions. Examples of such platforms include PayPal, Stripe, and Square.

Subscriptions refer to a business model where consumers pay a regular, recurring fee, usually on a monthly or annual basis, to gain ongoing access to a product or service. This model is widely used across various sectors, including digital media, software, and entertainment. Subscriptions provide customers continuous access to premium content, services, or products.

Digital payment platforms and subscription models are frequently integrated. The platforms automate the collection of recurring payments, thereby simplifying financial transactions for both service providers and subscribers.

Digital platforms have made financial transactions more accessible, but as a result, they are potentially more prone to exploitation. Recurring payment transactions, for example, can often go undetected as they are commonplace on many people's bank statements.

Perpetrator Behaviour

- *Subscriptions and Digital Payments:* Perpetrators may sign victims up for subscription services or recurring payments without their knowledge, draining their financial resources over time.

- *Digital Wallet Exploitation*: Platforms like PayPal or mobile payment apps can be misused to send money to the perpetrator's accounts, often hidden among legitimate transactions.

Practitioner Quick Action Response

- If the victim has passwords saved in browser accounts (e.g. Safari, Google Chrome, Microsoft Edge), which the perpetrator could access, the victim should either delete the saved passwords or remotely sign out of the associated accounts on devices the perpetrator could use.

- Once signed out, the victim should change their passwords and security questions, including to their iCloud/Google/Microsoft account.

Unauthorised Use of Online Banking and Shopping Accounts

Online banking refers to the provision of banking services through the internet, allowing customers to access and manage their bank accounts remotely. Users can check balances, transfer funds, pay bills, and even apply for loans or credit, all via a secure digital interface provided by their bank. This service offers the convenience of 24/7 access to financial information and transactions, reducing the need for in-branch visits.

Shopping accounts are user profiles created on e-commerce platforms or online retail websites. These accounts store personal information such as addresses, payment details, and purchase history, enabling a more personalised and efficient shopping experience. With a shopping account, customers can streamline the checkout process, track their orders, make wish lists, and view tailored product recommendations.

In a domestic abuse context where an older adult is the victim, online banking and shopping accounts can be exploited in several harmful ways:

Perpetrator Behaviour

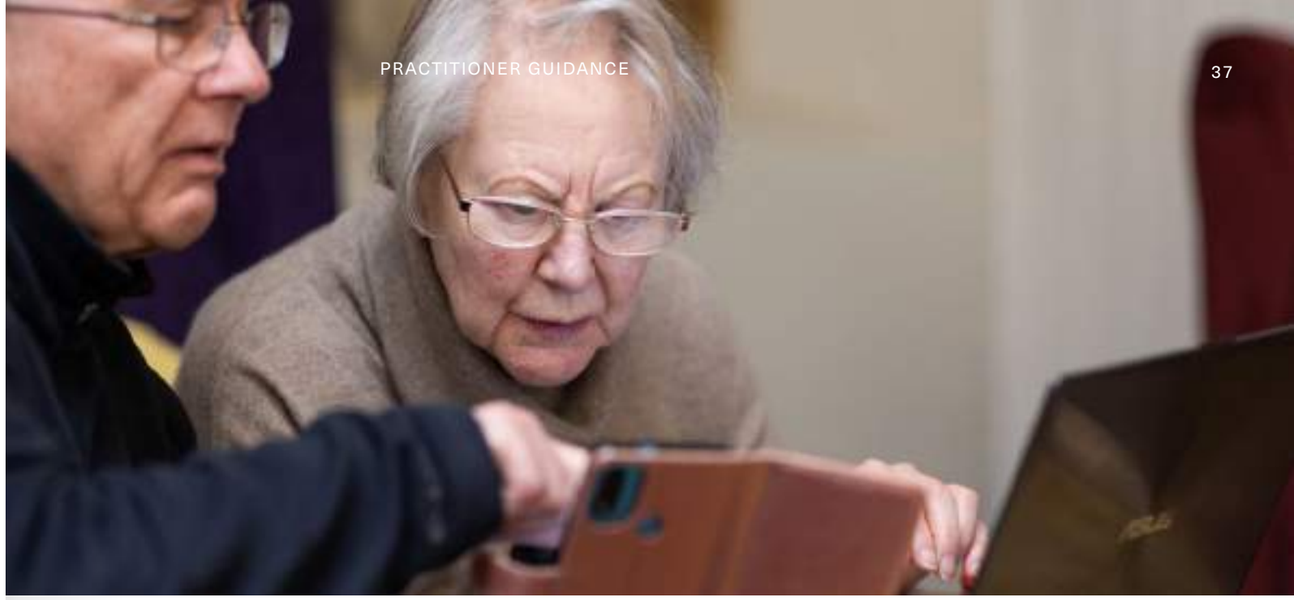
- *Make Unauthorised Transactions:* Perpetrators might use saved login credentials to transfer money, make purchases, or deplete the victim's savings. These transactions may appear routine or disguised as legitimate household spending, making them harder for victims to detect.

- *Restrict Financial Autonomy:* By changing passwords, removing victims' access, or transferring control of accounts to their own names, perpetrators can effectively eliminate the victim's ability to manage their finances independently.

- *Monitor Financial Activity:* Perpetrators may track spending habits or set up alerts for transactions, using this information to exert control or manipulate the victim into feeling incapable of managing their finances.

- *Manipulation of Financial Records:* Abusers can alter or delete transaction histories, which makes it difficult for the victim to track their spending or prove financial abuse.

- *Identity Theft and Data Exploitation:* Perpetrators may misuse stored payment details and personal information from shopping accounts, and perpetrators may commit identity theft.



Practitioner Quick Action Response

- Encourage victims to review their financial transactions regularly. Help in identifying unusual spending patterns or transfers that may indicate abuse/exploitation has occurred.

- Support victims in obtaining bank statements to assess any unfamiliar transactions. This will also begin gathering evidence for potential future criminal cases. It may be helpful to consult 'Understanding the Legal Framework' in this guide, to bolster your knowledge of the law and your ability to identify when a crime has occurred and share this understanding with the victim.

- Report abuse or fraud to the appropriate authorities i.e. bank retailers, police, Action Fraud.

- Remove saved payment details (such as bank cards) and linked accounts (such as PayPal) from online shopping sites to prevent funds being used to pay for goods and services. If this is not possible (due to the online account in question being controlled by another party) consider reporting to the bank to cancel payment cards and issue new ones. If recurring payments are set up on a bank card these can be stopped by contacting the card issuer.

- If a victim believes their account has been hacked (unauthorised access), they should notify their bank, change their password and security questions and answers immediately, and ensure 2 Step Verification is activated (usually automatic for banking). Victims can protect themselves by using fake or non-obvious answers to memorable security questions, making it harder for perpetrators to gain unauthorised access. Unless essential, truthful security answers are not required.

- Organisations such as MoneyAdvicePlus can offer help in cases of financial abuse, as well as provide assistance establishing disassociation orders.

Case in Practice: Unauthorised Use of Online Shopping Accounts

Keith, aged 67 years

Keith lived in his own home with his adult son while managing a terminal illness. He was proficient and confident in using digital technologies, including smartphones and online shopping accounts. At times, his son asked permission to purchase items using Keith's accounts, which Keith consented to by sharing his passwords. However, without Keith's knowledge or consent, his son continued to use the account to make unauthorised purchases.

How Technology Was Misused:

- Keith's son used saved passwords and account access to make repeated unauthorised purchases.
- Even after Keith changed his password multiple times, his son exploited security questions to reset the account credentials.
- Keith's son spent over £20,000 of Keith's money without permission.
- When confronted, Keith's son responded with physical and verbal aggression and caused damage to Keith's property.

Intervention and Support:
Keith was supported to:

- Report the incident to the police, which resulted in his son's arrest and a charge of criminal damage. As Keith's son was living with him at this point, a safety plan, including a restrictive order, was put in place to ensure his son did not return to the property.
- Secure his finances and online accounts with guidance on stronger security measures such as two-factor authentication and changing security questions.
- Restrict access to online shopping platforms, ensuring his son could no longer exploit his accounts.

Key Considerations for Practitioners:

- Even those who feel in control of their online security may be at risk from more digitally literate perpetrators.
- Password protection alone may not be sufficient. Practitioners should encourage the victims to use multi-factor authentication, change security questions, and ensure exclusive control over email recovery options.
- Emotional impact of economic abuse: although Keith was not in financial hardship, he was deeply affected by the loss of money he had planned to leave for his children. Economic abuse extends beyond immediate financial loss and can cause significant emotional distress.
- Police intervention and legal support: in cases where financial abuse escalates to physical threats or property damage, victims may need both safeguarding and legal intervention.
- Consider who also lives at the home of the older person you are supporting, as these factors may influence their safety when reporting abusive behaviours.
- Following on from this, further support may be required to establish a restrictive order once the perpetrator has been removed from the property.

This case demonstrates the ongoing risks of technology-assisted financial abuse, particularly when perpetrators have access to digital accounts and knowledge of security weaknesses. Practitioners can play a crucial role in supporting victims to regain financial independence and prevent further exploitation.

Coercive Control Under the Guise of 'Help'

Perpetrators of abuse could potentially exploit the victim's reliance on them for technological assistance, framing financial and digital abuse as legitimate help and support. These behaviours are often well-concealed and difficult for older adults and practitioners to identify, emphasising the importance of building confidence in older people and supporting them in developing technical proficiency.

Perpetrator Behaviour

- *Pretending to 'Fix' Errors:* Perpetrators may falsely claim that there are issues with the victim's accounts (e.g., "I noticed something suspicious and fixed it for you") to conceal unauthorised changes or transfers they made themselves.

- *Taking Over Technology Assistance:* Older victims may often require help setting up devices or apps. Perpetrators might capitalise on this opportunity to gain long-term access to financial accounts, ensuring ongoing control.

- *Taking Charge of Online Banking:* Small transactions that fall under the radar or significant financial behaviour.

- Misrepresenting Online Security Threats: Perpetrators may claim the victim's devices or accounts have been hacked, convincing them to hand over access for 'protection' while securing control over their information.

- *Deliberately Misleading or Confusing the Victim:* Perpetrators may use complex technical jargon or provide false explanations to discourage the victim from questioning financial transactions or technology-related changes.

- *Withholding or Controlling Passwords:* Perpetrators may insist on setting up passwords 'for security' but then withhold them from the victim, ensuring they remain dependent on the perpetrator for access.

- *Setting Up Automatic Payments to Themselves:* The perpetrator may establish standing orders or direct debits from the victim's account under the guise of handling their finances responsibly.

- *Monitoring Financial Activity Without Consent:* Perpetrators may set up alerts for financial transactions or use digital banking features to track spending, reinforcing control over the victim.

- *Exploiting Online Shopping or Subscription Services:* The perpetrator may use the victim's stored payment details for their own purchases, often under the pretext of helping the victim manage their accounts.

- *Preventing the Use of Cash or Alternative Payment Methods:* Perpetrators may discourage or prevent older victims from using cash or in-person banking, forcing them into digital transactions they cannot control independently.

- *Tampering with Assistive Technology or Smart Devices:* For older victims using assistive technology (e.g., voice-activated devices, home monitoring systems), perpetrators may manipulate settings to create confusion, enforce isolation, or reinforce control.

- *Blocking Access to Banks:* Perpetrators may monitor phone calls or emails, intercept bank correspondence, or discourage the victim from visiting their bank in person, ensuring that only the perpetrator has direct communication with financial services.

- *Next Day Delivery:* Perpetrators may offer to place orders for the victim using their own shopping accounts, claiming it will provide benefits like free delivery. However, they may then save the older victim's card details on their account for future unauthorised use.

These perpetrator behaviours illustrate how coercive control can be masked as "help" and highlight the importance of digital literacy, financial independence, and practitioner awareness in safeguarding older victims.

Key Considerations for Practitioners

- Safety planning is instrumental in reducing the risk of escalation from the perpetrator.

- Practitioners should assess the victim's digital vulnerabilities, including who has access to their online banking, email, and personal accounts.

- Providing practical support, such as guiding victims through resetting passwords, setting up new accounts, and monitoring for fraudulent transactions, is essential in restoring financial independence.

- Create lists of trusted contacts for banks and service providers to support the victim to contact those organisations directly for assistance, instead of relying on the perpetrator.

Case in Practice: Technology-Assisted Economic Abuse

Janice, aged 72 years

Janice confided in a nurse at her GP surgery that she was unhappy living with her son and daughter-in-law. When the nurse inquired further, Janice explained that she was worried about money and felt she had lost her independence. Her son had set up digital banking on her behalf, and she had no access to her finances. She had not seen a bank statement for two years and had no idea how much money was in her account.

How Technology Was Misused:

- Janice's son had taken control of her digital banking, preventing her from accessing her own financial information.
- He withheld bank statements, leaving Janice unaware of her financial situation.
- When Janice asked to see details of her bank account, her son became angry, making her afraid to ask again.

Intervention and Support:
Janet was supported to:

- Secure independent housing, enabling her to regain control over her daily life.
- Visit her bank to remove her son's access to her account and issue her with a new debit card.
- Review her financial records, where she discovered that her son had been withdrawing her pension and savings without her knowledge.

Safety Note:

To reduce the risk of repercussions from the perpetrator, actions taken to secure Janet's bank account were delayed until she had moved out of the perpetrator's home.

Janice's case highlights how digital tools can be weaponised in economic abuse and reinforces the importance of digital safeguarding measures in supporting older victims of coercive control.

Intimate Image-Based Abuse

Image-based abuse refers to the non-consensual creation, sharing, or threat of sharing intimate or explicit images or videos to control, coerce, humiliate, or punish a victim (Dragiewicz et al., 2018; Lever and Eckstein, 2020). This form of technology-facilitated abuse is often used by perpetrators in cases of domestic abuse, coercive control, and post-separation abuse.

Forms of Image-Based Abuse in Domestic Abuse Cases:

1. Non-Consensual Sharing of Intimate Images

- A perpetrator distributes private sexual images or videos of the victim without their consent.
- This could involve sharing the content with friends, family, colleagues, or online platforms, causing distress and reputational harm.
- Often referred to as 'revenge porn', but more accurately described as intimate image abuse, as it is not always motivated by revenge.

2. Threats to Share Intimate Images

- The threat to disclose explicit images, even if they are never actually shared, can be a powerful tool of coercion and control.
- Victims may comply with demands for money, continued contact, or sexual acts due to fear of exposure.
- Covered under Section 69 of the Domestic Abuse Act 2021, which criminalises the threat to disclose intimate images as a standalone offence.

3. Coerced or Secretly Taken Images

- Perpetrators may pressure, manipulate, or force victims into sending explicit photos (often under the pretext of trust or affection).
- Some perpetrators may covertly record sexual activity or secretly take intimate photos, later using them as blackmail or a tool of control.

4. Editing and Misuse of Images

- Technology allows perpetrators to manipulate or create fake explicit images using deepfake technology or AI-generated content.
- Victims may be falsely accused of appearing in sexual material, furthering psychological abuse and reputational damage.

Key Considerations for Practitioners

- Validate the victim's experience in a non-judgemental manor. Support with emotional and legal guidance, helping victims report the abuse to police, online platforms, or victim support services.
- Encourage digital safety measures, such as recovery of hacked accounts, reviewing privacy settings, and removing stored images from cloud backups.
- Recognise that threats alone constitute abuse and victims do not need to experience the distribution of intimate images for this to be harmful.
- Report or assist the reporting of harmful/illegal images.

Understanding the Legal Framework

Older adults who have been subjected to technology-facilitated abuse may not recognise that they have been the victim of a crime (or what help is available for them). By familiarising themselves with key legislation, practitioners can better identify criminal behaviours, inform victims of their rights, and advocate for their safety and justice. The following laws are particularly relevant when addressing technology-facilitated domestic abuse and economic crime in the context of older victims, enabling practitioners to guide victims effectively through the reporting process.

Computer Misuse Act 1990

The Computer Misuse Act 1990 addresses unauthorised access to devices and data. It criminalises acts such as hacking, installing spyware, or accessing an individual's email accounts, banking apps, or smart devices without permission.

Relevance to Practitioners

Practitioners working with older victims should be aware that unauthorised access to a device or data is a criminal offence, even if the perpetrator is a family member or partner. Victims may feel reluctant to report such behaviour, particularly if they perceive it as a domestic matter. Practitioners can reassure victims that the law recognises these actions as serious crimes and encourages them to report incidents to the police. Furthermore, understanding the provisions of this act enables practitioners to identify potential signs of computer misuse, such as if the rightful user is reporting unexpected activity on devices, unexplained changes to account settings, or the installation of unfamiliar software.

Protection from Harassment Act 1997

Stalking and harassment are covered under the Protection from Harassment Act 1997 and Section 42A (1) of the Criminal Justice and Police Act 2001 (harassment of a person in their home).

The Protection from Harassment Act 1997 legislation covers repeated behaviours, including online stalking and harassment, which cause distress or fear. The Act is particularly relevant in cases where technology is used to facilitate controlling or threatening behaviour, such as persistent messaging, monitoring via GPS, or stalking through social media. Behaviors can include online harassment, cyberstalking, and persistent unwanted digital communication.

Relevance to Practitioners

Harassment can be described as persistent tracking or unwanted communication, and victims can sometimes find it difficult to articulate how these behaviours manifest. Practitioners should help older victims identify patterns of harassment, including behaviours that may not initially seem linked. Guiding victims in collecting evidence, such as screenshots of messages, records of suspicious emails, or documentation of device tracking, is crucial when pursuing criminal justice. By recognising the protections afforded under this act, practitioners can empower victims to seek protection orders or police intervention to halt harassing behaviours.

Fraud Act 2006

The Fraud Act 2006 targets deceptive practices, including impersonation scams, phishing attacks, and other forms of financial exploitation.

Relevance to Practitioners

As discussed above, for older victims, these behaviours can often be disguised as assistance from the perpetrator. Practitioners' efficacy in these situations will greatly benefit from their knowledge of the provisions of this act, allowing them to identify fraudulent activity against the victim.

By understanding the provisions of this Act, practitioners can guide victims to report fraudulent activity to Action Fraud, the UK's national reporting centre for fraud and cybercrime.

Domestic Abuse Act 2021

The Domestic Abuse Act 2021 expanded the legal definition of domestic abuse to include controlling or coercive behaviour, even when facilitated through technology. The Act recognises that behaviours such as monitoring devices, restricting access to financial resources, or isolating a victim digitally can be aspects of domestic abuse.

Relevance to Practitioners

Practitioners can use the framework of this Act to validate victims' experiences and highlight that these actions are recognised forms of abuse by law. Older victims may not be aware that technology-facilitated abuse is recognised as domestic abuse and can be reported to the police.

By understanding these laws and their practical applications, practitioners can effectively support older victims of domestic abuse, ensuring they are informed, protected, and empowered to seek justice. Familiarity with the legal framework also enables practitioners to collaborate more effectively with law enforcement, legal services, and other organisations, fostering a comprehensive response to technology-facilitated abuse and economic exploitation. This can include sharing explicit images online, threats via messages, or uploading images to adult websites without consent.

- Section 69 of the Domestic Abuse Act 2021 makes it an offence to threaten to disclose explicit images.

- Section 33 of the Criminal Justice and Courts Act 2015 covers the actual disclosure of intimate images with intent to cause distress.

Family Law Act 1996

Section 63 of the Family Law Act 1996 defines a relative as:

'(a) the father, mother, stepfather, stepmother, son, daughter, stepson, stepdaughter, grandmother, grandfather, grandson or granddaughter of that person or of that person's spouse, former spouse, civil partner or former civil partner.'

Or '(b) the brother, sister, uncle, aunt, niece, nephew or first cousin (whether of the full blood or the half blood or by marriage or civil partnership) of that person or of that person's spouse, former spouse, civil partner or former civil partner'.

Section 63 also adds that relatives include 'in relation to a person who is cohabiting or has cohabited with another person, any person who would fall within paragraph (a) or (b) if the parties were married to each other or were civil partners of each other.'

Relevance to Practitioners

The Family Law Act 1996 provides the definition of a 'relative' for the purpose of the Domestic Abuse Act 2021.

Serious Crime Act 2015: Coerciveor Controlling Behaviour

Section 76 of the Serious Crime Act 2015 introduced the criminal offence of coercive or controlling behaviour in an intimate or familial relationship. Coercive or controlling behaviour consists of patterns of abusive behaviour, which may include the use of technology.

The coercive or controlling statutory guidance framework issued section 77 of the Serious Crime Act 2015 outlines a number of methods that can be used to record evidence of technology-facilitated abuse.

Relevance to practitioners

The guidance is aimed at statutory and non-statutory bodies working with victims, perpetrators, and commissioning services. The statutory guidance emphasises the importance of gathering evidence in a timely manner, including the retrieval of perpetrator's devices to reduce the opportunity for perpetrators to delete or destroy evidence, provide the wrong devices, or password-protect their devices.

Collecting Evidence on Technology-Facilitated Abuse

The coercive or controlling statutory guidance framework issued under section 77 of the Serious Crime Act 2015 outlines a number of methods that can be used to record evidence of technology-facilitated abuse. The guidance is aimed at statutory and non-statutory bodies working with victims, perpetrator and commissioning service.
The methods of recording evidence include:

- Phone records (whilst ensuring limited disruption, if any, for the victim, ensuring appropriate redaction and not risking further harm).
- Text messages (whilst ensuring limited disruption, if any, for the victim, ensuring appropriate redaction and not risking further harm).
- Device logs (whilst ensuring limited disruption, if any, for the victim, ensuring appropriate redaction and not risking further harm).
- Evidence of abuse over the internet, digital technology (e.g. smart speakers) and social media platforms.
- Copies of emails.
- Bank records to show financial control.
- Abusive postings on public platforms, including social media diary kept by the victim.
- GPS tracking devices installed converted and/or overtly on mobile phones, tablets, vehicles etc.
- Where the perpetrator has a carer responsibility, the care plan might be useful as it details what funds should be used for – e.g. caring for a child, caring for a parent or a sibling.
- CCTV and home video footage e.g. smart doorbells.
- Device logs.
- Keep evidence that something was installed on the device, take a screenshot and store it somewhere safe.

The collection of evidence should ensure limited disruption, if any, for the victim, ensuring appropriate redaction and not risking further harm.

There are a number of helpful apps that victims can be encouraged to use to safely and legally record evidence. For example, Kulpa is an internationally accredited app that can document what happened, when and where (ISO/IEC 270001). Any data captured or uploaded in the app is safely secured on Kulpa's secure cloud servers. Victims can choose to submit the evidence recorded to the police or another third party via the app or delete the data (which cannot be retrieved).

The statutory guidance emphasises the importance of gathering evidence in a timely manner, including the retrieval of perpetrators' devices to reduce the opportunity for perpetrators to delete or destroy evidence, provide the wrong devices, or password-protect their devices.

Case in Practice: Dyfed-Powys Police - Katherine

Katherine had been in a relationship with Steven for a period of six months. During this time, he tried to isolate her from friends and family by encouraging her to remove herself from social media platforms so that she was unable to communicate with others.

Steven was extremely jealous of Katherine. One night whilst out with a friend, Steven persistently rang her on her mobile phone and tracked her on Life360. Feeling pressured, Katherine returned home. It was at that time Steven examined her mobile phone without her consent and her social media pages. Steven found communication between Katherine and another male named Billy, although the content of this communication was not known.

Steven set up a fake Facebook account in Katherine's name, purported to be her and used this to communicate with Billy. Steven identified that during Katherine's night out she had talked to Billy about her relationship with Steven. At this point Steven's behaviour escalated and he seriously assaulted Katherine.

How Technology Was Misused:

- Steven forced Katherine to share her usernames and passwords with him. Steven exerted pressure on Katherine to do this, misleading her into believing that it was for her own wellbeing and for him to help her out with any important correspondence that might need replying to. Katherine used the same passwords across multiple platforms.

- Steven created a fake Facebook account using Katherine's details, to deceive Billy into believing he was communicating with her. Steven read these messages.

- Steven was using Life360 to track Katherine's movements.

Good Evidence Gathering

- When police attended Katherine's home address to arrest Steven, they utilised Golden Hour principles to secure as much forensic and digital material as possible.

- Both Steven and Katherine's mobile devices were secured, to safeguard Katherine from further harm and to limit further disruption, she was provided with a handset that had various safety apps on, such as Hollie Guard and Refuge.

- A forensic download of both mobile devices was conducted, with Katherine's device taking precedence, to limit her being without it for longer than necessary.

- Phone records and text messages were requested that identified the obsessive behaviour by Steven towards Katherine, where on some occasions he would telephone her up to 100 times a day and send her abusive and controlling texts.

- A police search of the premises identified a Ring door bell camera at the premises, which was covertly placed in the shed, to record any visitors to the house. The camera was identified through a thorough search. The corresponding app to control the camera was located on Steven's mobile phone, evidencing how his fixated and obsessive behaviour limited and controlled Katherine's interactions with others.

- Social Media data was obtained for both Katherine's legitimate account and the fake profile created by Steven. This data identified a clear pattern to Steven's offending. The prosecution could assert that when Katherine started dating Steven her social media presence declined rapidly. The fake account was being used to not only communicate with Billy but with other associates and friends of Katherine's, whereby Steven would tell her friends that she was taking a hiatus from social media for a bit. Steven also changed the mobile number linked to Katherine's profile so that he could intercept any calls and messages.

- Suitable guidance and safeguarding were provided to Katherine, relating to improving online security and improving digital awareness and hygiene.

- This collection of evidence assisted in supporting the prosecution in building a case that highlighted Steven's behaviour, which consisted of coercive and controlling behaviours as well as both physical and mental abuse and stalking. The digital data was presented successfully and Stephen was convicted at court after his actions.

Protective Conditions & Provisions to Prevent Offending

There are several legal conditions and protective measures that can help prevent further technology-facilitated abuse:

Restraining Order
Prevents contact via phone, email, or social media. May restrict indirect contact through third parties.

Non-Molestation Order
Can include prohibitions on online harassment, including messaging and social media contact.

Bail Conditions
May include restrictions on electronic communication or contact via digital platforms.

Domestic Abuse Protection Order (DAPO)
Can restrict digital surveillance, prevent access to certain technology, or prohibit online threats.

Stalking Protection Order
Can ban the use of tracking software, restrict access to victims' social media, and prevent online harassment.

Important:
This is not an exhaustive list of offences or protective conditions. The aim is to enhance awareness so that practitioners can help victims prevent further harm through appropriate legal measures.

Resources

- Action Fraud UK – *www.actionfraud.police.uk*
- Age Cymru offer computer training courses for older people. These courses are accessible for all, and the website offers tools to locate the nearest centre available to attend their courses – *https://www.ageuk.org.uk/services/in-your-area/it-training/*
- Information which has been developed for GPs to share with patients – *https://digital.nhs.uk/services/nhs-app/toolkit/see-your-gp-health-record-in-the-nhs-app*
- Irisin guidance to GP practices around the changes to the NHS app and how to manage this to safeguard victims and survivors – *https://irisi.org/changes-online-medicalrecords-gp/*
- Kulpa – *https://www.kulpacloud.com*
- Money Advice Plus – *https://www.moneyadviceplus.org.uk/*
- NCSC (National cyber security centre) – *https://www.ncsc.gov.uk*
- Refuge – *https://refuge.org.uk*
- Revenge Porn Helpline – *www.revengepornhelpline.org.uk*
- South End and Thurrock Domestic Abuse Partnership (SETDAB). It's never too late campaign – *https://setdab.org/resource/setdab-its-never-too-late-campaign-2025/*
- Spot the AI Interactive learning – *https://www.getsafeonline.org/spottheai/*
- Surviving Economic Abuse, in partnership with Money Advice Plus, collaborated to create a guide on understanding economic abuse – *https://survivingeconomicabuse.org/news/sea-launches-digital-guide-to-helpvictims-identify-economic-abuse/*

References

Age UK. (2023). "You can't bank on it anymore": *The impact of the rise of online banking on older people* [online], available at: https://www.ageuk.org.uk/siteassets/documents/reports-and-publications/reports-and-briefings/money-matters/the-impact-of-the-rise-of-online-banking-on-older-people-may-2023.pdf

Bishop, C. and Bettinson, V. (2018) *Evidencing domestic violence*, including behaviour that falls under the new oVence of 'controlling or coercive behaviour'.* The International Journal of Evidence & Proof, 22(1), pp.3-29

Brookfield, K., Fyson, R. and Goulden, M. (2023) *Technology-Facilitated Domestic Abuse: an under-Recognised Safeguarding Issue? British Journal of Social Work,* 54(1). doi: https://doi.org/10.1093/bjsw/bcad206

Bünning M, Schlomann A, Memmer N, Tesch-Römer C, Wahl HW. *Digital Gender Gap in the Second Half of Life Is Declining: Changes in Gendered Internet Use Between 2014 and 2021 in Germany*. J Gerontol B Psychol Sci Soc Sci. 2023 Aug 2;78(8):1386-1395. doi: 10.1093/geronb/gbad079. PMID: 37218293; PMCID: PMC10394992

Carers UK. (2023) *Supporting older carers who are digitally excluded: A good practice briefing [online]*, available at: https://www.carersuk.org/media/ednddumI/supporting-older-carers-who-are-digitally-excluded-briefing.pdf (Accessed: 20 February 2025)

Christie, L. and Wright S. (2020) *Technology and Domestic Abuse* [online], London, UK Parliament DOI: hVps://doi.org/10.58248/RR51

Computer Misuse Act 1990

Criminal Justice and Courts Act 2015

Cuomo, D. and Dolci, N. (2021) *New tools, old abuse: Technology-enabled coercive control (TECC)*. Geoforum, 126, pp.224-232

Domestic Abuse Act 2021 (England and Wales)

Dragiewicz, M., Burgess, J., Matamoros-Ferna´ndez, A., Salter, M., Suzor, N., Woodlock, D. and Harris, B. (2018) *'Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms', Feminist Media Studies,* 18(4), pp. 609–25

Fallows, D. (2005). *How Women and Men Use the Internet.* [online] Pew Research Centre. Available at: https://www.pewresearch.org/internet/2005/12/28/how-women-and-men-use-the-internet/ (Accessed: 24 February 2025).

Family Law Act 1996 (England and Wales)

Fraud Act 2006

Freeman, E. (2022) *'How effective are the protections available in Wales to safeguard adult victims of "coercive or controlling behaviour" by an intimate/ex-intimate partner or adult family member?'*, Dissertation for partial completion of MA Safeguarding Adults: Law, Policy and Practice, School of Law, Keele University

Goodthingsfoundation.org. (2024) *Solving Digital Exclusion in a Cost of Living Crisis | Good Things Foundation.* [online] Available at: https://www.goodthingsfoundation.org/policy-and-research/research-and-evidence/research-2024/solve-digital-exclusion-cost-of-living-crisis (Accessed: 21 February 2025).

Haase, K.R., Cosco, T., Kervin, L., Riadi, I. and O'Connell, M.E. (2021) *Older adults' experiences with using technology for socialization during the COVID-19 pandemic: Cross-sectional survey study. JMIR aging, 4*(2), p.e28010

Harris, B. and Woodlock, D. (2018) *'Digital coercive control: Insights from two landmark domestic violence studies', The British Journal of Criminology,* 59(3), pp. 530–50

Independent Age. (2024). *New data shows online scams cost older people an average of £4,000: but financial loss is only part of the story.* [online] Available at: https://www.independentage.org/news-media/press-releases/new-data-shows-online-scams-cost-older-people-an-average-of-ps4000-but (Accessed: 5 August 2025).

Kelly, L. (1988) Surviving Sexual Violence. Cambridge: Polity.

Leitao, R. (2021) *'Technology-facilitated intimate partner abuse: A qualitative analysis of data from online domestic abuse forums', Human–Computer Interaction,* 36(3), pp. 203–42.

Lever, K. and Eckstein, J. (2020) *'"I never did those things they said!": Image, coercive control, and intrusion from former partners' technology-mediated abuse', Iowa Journal of Communication,* 52(1), pp. 49–67

Lopez-Neira, I., Patel, T., Parkin, S., Danezis, G. and Tanczer, L. (2019) *''Internet of Things': How Abuse is Getting Smarter', Safe – the Domestic Abuse Quarterly,* 63, pp. 22–26

NHS England. (2023) *NHS App reaches record users on fifth anniversary, 27th December 2023,* [online] https://www.england.nhs.uk/2023/12/nhs-app-reaches-record-users-on-fifth-anniversary/ (Accessed: 23 January 2024)

Older People's Commissioner for Wales. (2017) *Information and guidance on domestic abuse: Safeguarding older people in Wales* [online] available at: https://www.gov.wales/sites/default/files/publications/2019-06/safeguarding-older-people-in-wales.pdf (Accessed: 20 February 2025)

Okun, L. (1986) *Woman abuse: facts replacing myths / Lewis Okun - Catalogue | National Library of Australia.* [online] Available at: https://catalogue.nla.gov.au/catalog/3001343

Protection from Harassment Act 1997 (England and Wales)

Refuge. (2021) *Unsocial Spaces: Make Online Spaces Safer for Women and Girls* [Online] available at: https://refuge.org.uk/wp-content/uploads/2021/10/Unsocial-Spaces-for-web.pdf

Santander Press Office. (2020) *Over 55s Flock Online during Coronavirus Pandemic but Miss Out on Digital Banking Opportunity | Santander UK.* [online] Available at: https://www.santander.co.uk/about-santander/media-centre/press-releases/over-55s-flock-online-during-coronavirus-pandemic-but (Accessed: 5 August 2025).

Serious Crime Act 2015 (England and Wales)

Smith, L. (2020) *Older People Still Wary of Online Banking.* [online] www.moneyexpert.com. Available at: https://www.moneyexpert.com/news/older-people-still-wary-of-online-banking/ (Accessed: 5 August 2025)

Stark, E. (2007) Coercive Control: *How Men Entrap Women in Personal Life.* New York: Oxford University Press.

Tabassum, N. (2020) *How are older people adapting to digital technology during the COVID-19 pandemic, Centre for Ageing Better.* Available at: https://ageing-better.org.uk/blogs/how-are-older-people-adapting-digital-technology-during-covid-19-pandemic (Accessed 1 May 2024)

Tanczer, L., Lopez Neira, I., Parkin, S., Patel, T., and Danezis, G. (2018) *Gender and IoT Research Report; the Rise of the Internet of Things and Implications for Technology-Facilitated Abuse* [Online], London, UCL. https://discovery.ucl.ac.uk/id/eprint/10140276/1/giot-report.pdf

Tanczer, L., Lo´ pez-Neira, I. and Parkin, S. (2021) *'I feel like we're really behind the game': perspectives of the United Kingdom's intimate partner violence support sector on the rise of technology-facilitated abuse', Journal of Gender-Based Violence,* 5(3), pp. 431–50

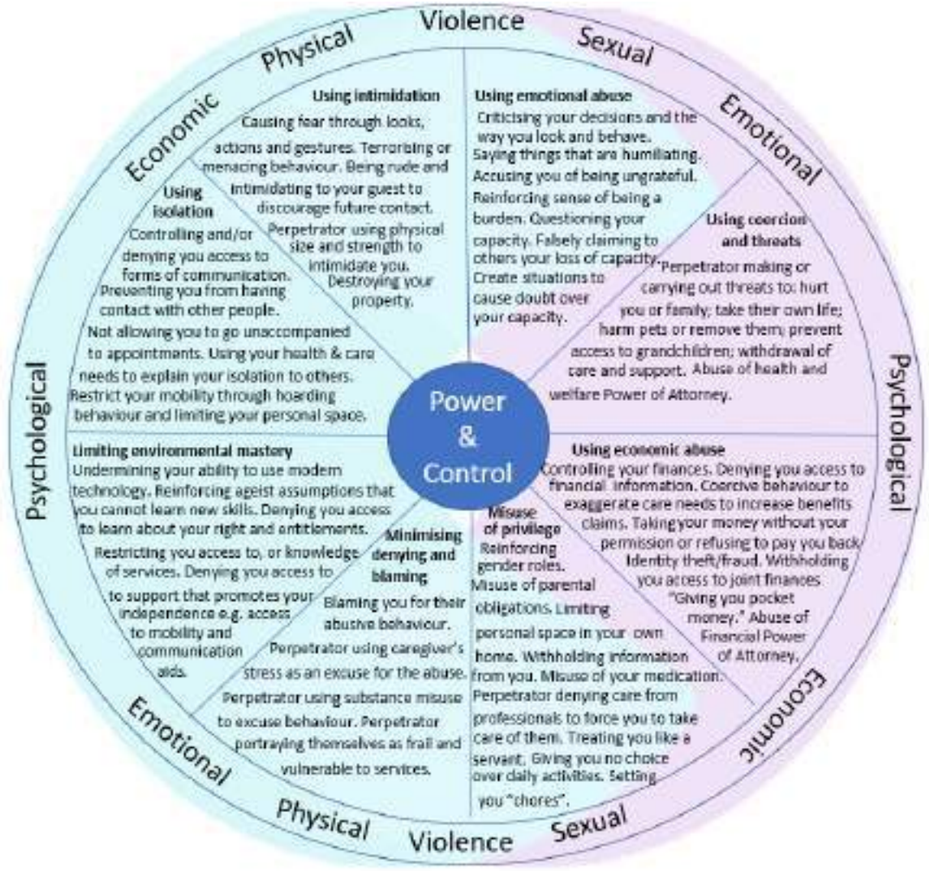
Vodafone UK News Centre. (2022) *Fear of going online could cost over 65s almost £1,000 a year.* [online] Available at: https://www.vodafone.co.uk/newscentre/news/fear-of-going-online-could-cost-over-65s-almost-1000-a-year/ (Accessed: 5 August 2025)

Women's Aid. (2023) *Criminalisation of coercive control reaches eight-year anniversary.* [online] Available at: https://www.womensaid.org.uk/criminalisation-of-coercive-control-reaches-eight-year-anniversary/ (Accessed: 5 August 2025)

Wydall, S., Freeman, E. and Zerk, R. (2021) *Transforming the response to domestic abuse in later life.* Gomer Press: Llandysul

Yardley, E. (2020) *'Technology-facilitated domestic abuse in political economy: A new theoretical framework', Violence against Women,* 27(10), pp. 1479–98.

Appendix A.
Domestic Violence and Abuse in Later Life



Dewis Choice have adapted the Power and Control Wheel to illustrate older people's experiences of domestic violence and abuse from intimate partners and adult family members. The Wheel has been developed based on the lived experiences of over 90 victim-survivors that have engaged with the Dewis Choice Initiative.

Glossary

1. **Accessibility:**
   The design of technology and services to ensure they can be used by all individuals, including those with disabilities or limited digital skills.

2. **Application:**
   A program or piece of software designed to fulfil a particular purpose.

3. **Digital Assistants:**
   Devices like Alexa or Google Home that can be used to issue commands.

4. **Digital Exclusion:**
   The inability, or limited ability, to access or use digital tools and the internet due to barriers like affordability, skills gaps, or confidence issues.

5. **Digital Literacy:**
   Capabilities that fit someone for living, learning, working, participating and thriving in a digital society.

6. **Digital Payment Platforms:**
   Digital infrastructure that enables the processing and facilitation of financial transactions.

7. **Golden hour Principles:**
   Refers to the critical period immediately following a crime where effective action can significantly impact the success of an investigation.

8. **GPS:**
   Global Positioning System.

9. **Hacking:**
   Gaining unauthorised access to devices or accounts to manipulate or control victims.

10. **ISO/IEC 27001:**
    Is the globally recognized international standard for Information Security Management Systems (ISMS).

11. **Location Sharing:**
    A smartphone or device feature that can be used to share one's accurate location to another.

12. **Misuse of Cloud Storage:**
    Accessing sensitive online files without consent, to intimidate, extort or manipulate an individual.

13. **Smart Home Devices:**
    Internet-connected tools like cameras, locks and assistants.

14. **Smart Locks:**
    Devices that can provide or deny them access to one's home remotely.

15. **Smart Thermostats:**
    Technology able to control home temperatures.

16. **Two-Step Verification (2SV)/ Multi Factor verification:**
    A security method to protect accounts by requiring a second layer of authentication.

17. **Unauthorised Transactions:**
    Financial activities, like transferring money or making purchases, conducted without the victim's consent.

18. **User-Friendly Interfaces:**
    Designs in technology that prioritise simplicity and ease of use, reducing barriers for older adults.

Heddlu Police
DYFED POWYS

1872 PRIFYSGOL ABERYSTWYTH UNIVERSITY

Dewis CHOICE

PEGS