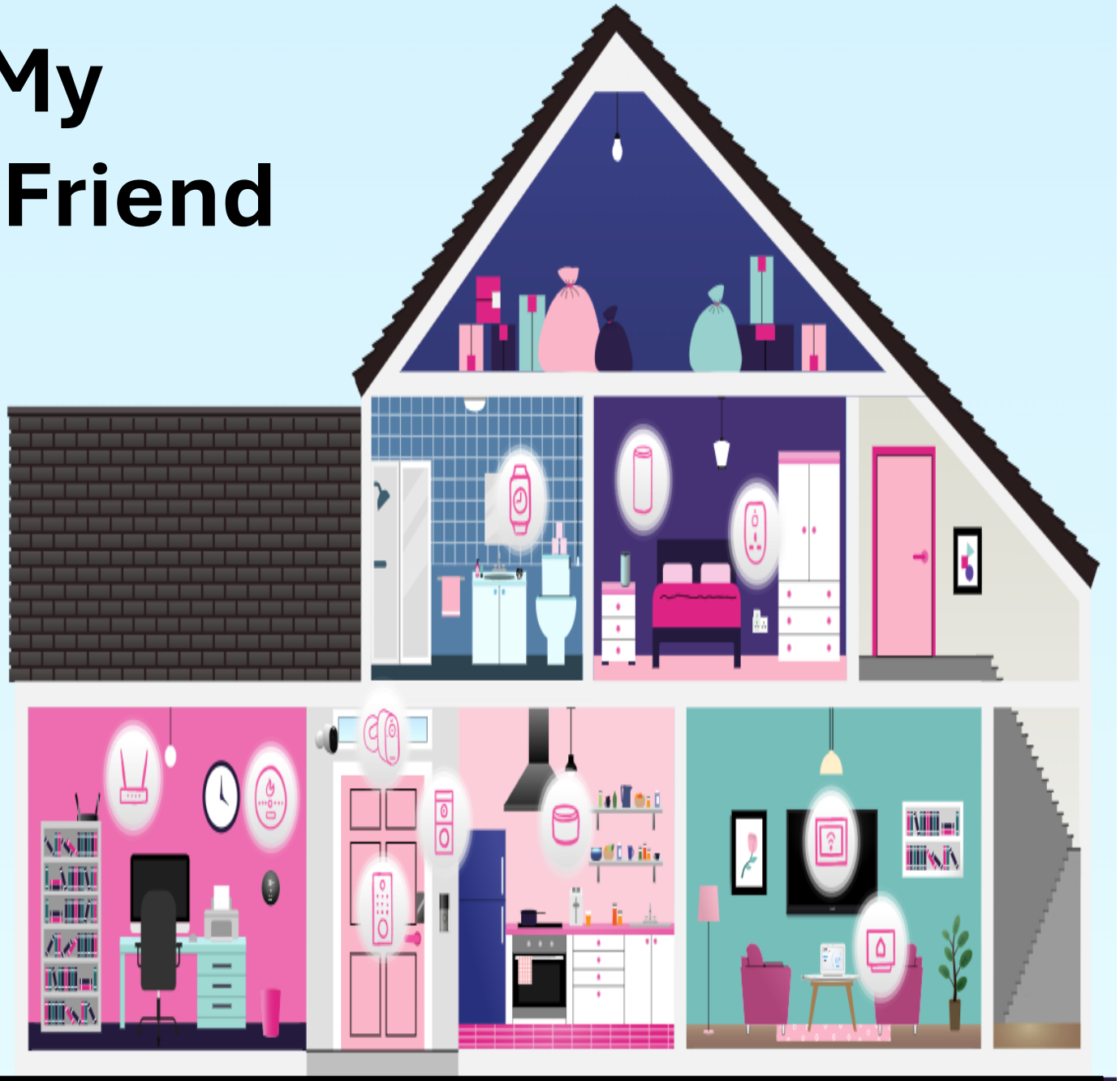
The Changing Landscape – Technology Facilitated Abuse

Support:

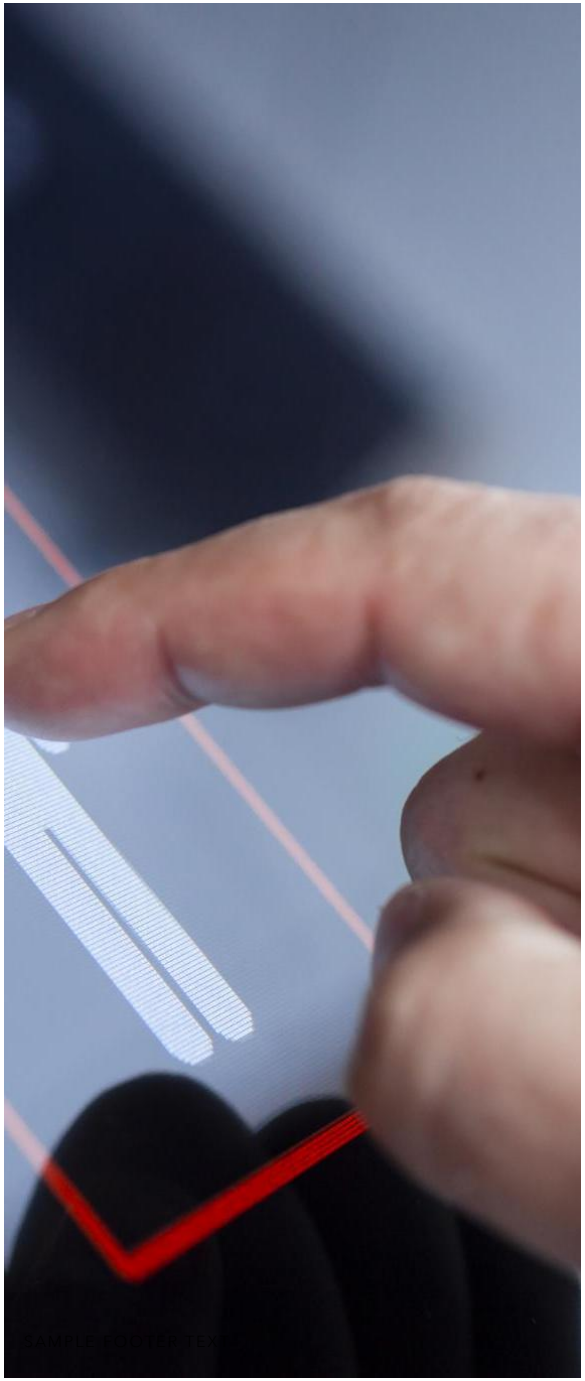
- https://www.suzylamplugh.org / stalking helpline
- https://refugetechsafety.org/
- https://refugetechsafety.org/digitalbreakup/
- https://refugetechsafety.org/secure-your-tech/
- https://refugetechsafety.org/hometech/
- UK's Home for Reporting Cyber Crime & Fraud - Report Fraud
- Revenge Porn Helpline - 0345 6000 459 | Revenge Porn Helpline

Tech in My Home – Friend or Foe?



Name as many digital & smart devices that you or someone else might have:

Slido.com
#3114 549



What is Tech Abuse?

Definition and Scope

Tech Abuse involves misuse of digital tools to harass, control, or intimidate individuals in various settings.

Technologies Involved

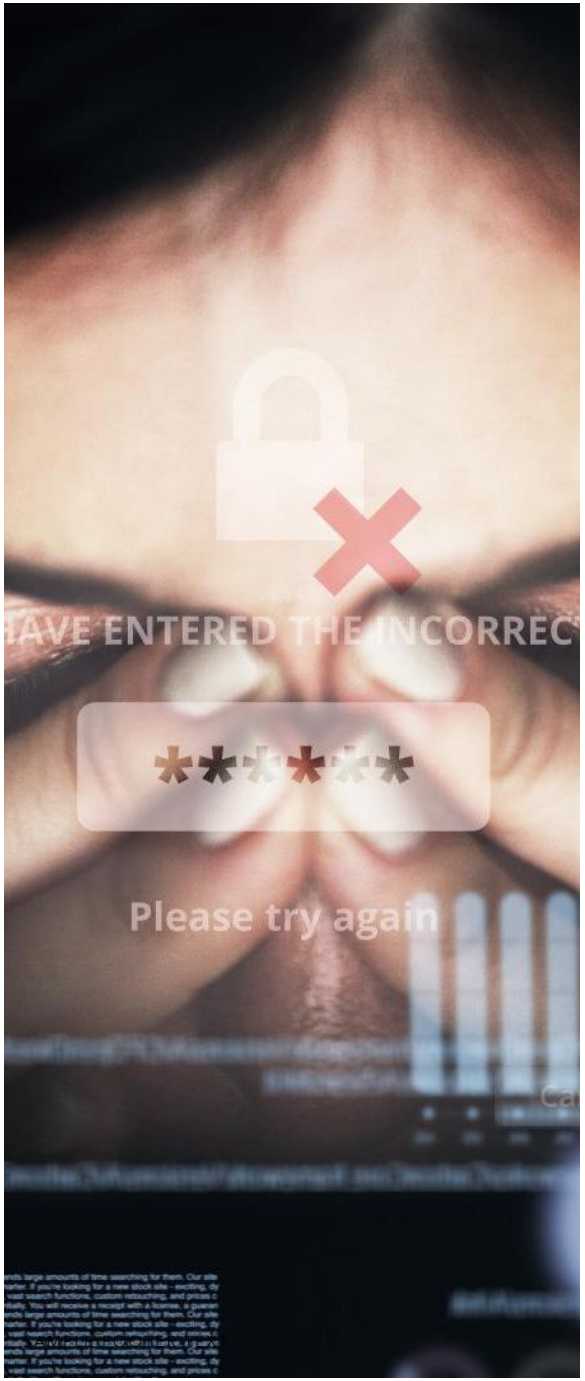
Abuse can occur through smartphones, TV's, cars, speakers, fridges, smoke detectors, computers, and emerging tech like AI-generated fake content.

Impact and Challenges

Tech Abuse causes psychological harm, amplifies coercive control, and is hard to detect and define universally.

Importance for Professionals

Understanding Tech Abuse aids practitioners in identifying and responding to abuse effectively.



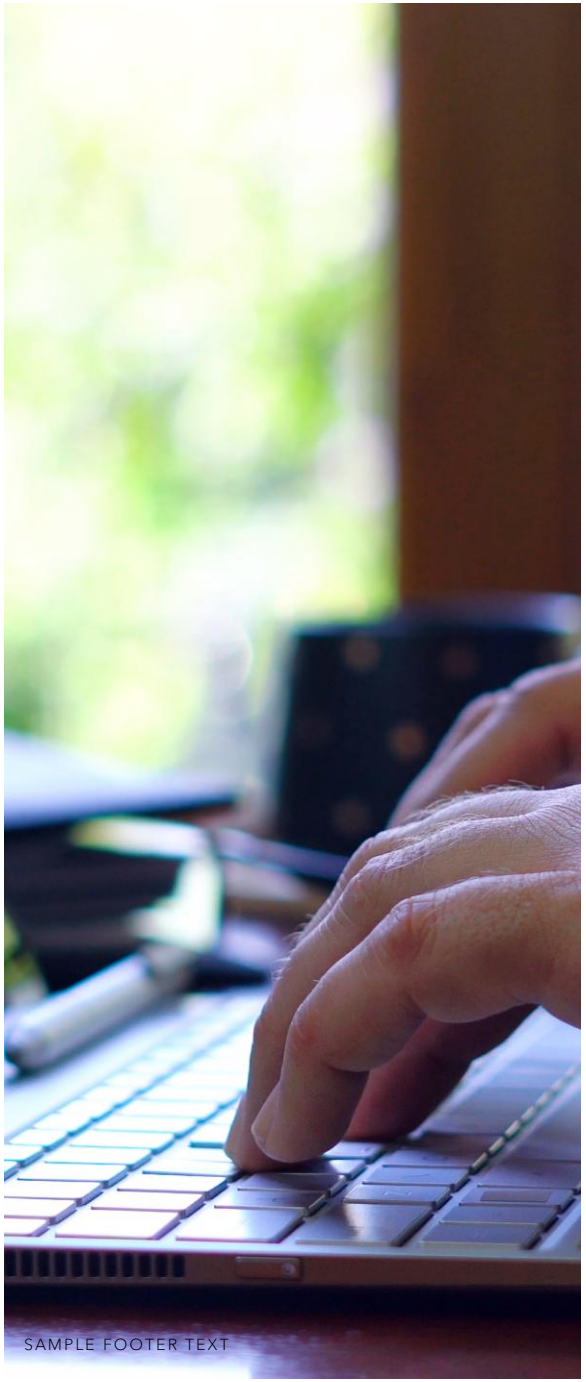
Prevalence and Impact

Rising Tech Abuse Cases

- Tech Abuse affects a growing number of victims. In 2023–24, **32%** of women contacting the UK National Domestic Abuse Helpline reported experiencing at least one form of Tech Abuse.
- Between **2018 and 2022**, Refuge recorded a **258% increase in technology-facilitated violence** among its clients.
- **Refuge reports a 62% rise in referrals for tech-facilitated abuse in 2025 compared to 2024**.
- **62%** of Domestic Abuse victims reported perpetrators creating fake accounts & **44%** experienced being tracked via devices (Changing Lives 2025)
- AI-driven abuse is surging: **95% of online deepfakes are non-consensual pornographic images**, and **99% target women**.

Cyberstalking Trends:

- Stalking (all forms) has increased by **75% in five years.**
- **80% of stalking victims are tracked using technology**.
- Nearly half of victims perceive cyberstalking as **"wrong but not a crime"**, which significantly reduces reporting rates



Prevalence and Impact

Domestic Abuse Data:

- 2025 (ONS data) 2.2 million females & 1.5 million males experienced domestic abuse
- 20% of young people 16 to 19 had experienced domestic abuse.
- Significant rise in coercive control, image-based abuse, and digital harassment for 16 -24 year olds

Digitally Enabled Coercive Control (DECC):

- Fundamentally impacted by technological advancement
- Makes coercive control more pervasive and easier to perpetrate.
- Removes the need for the victim and offender to occupy the same space, increasing the sense of abuser omnipresence
- Victim-survivors are now always contactable and can be subject to continuous monitoring

Common Tactics and Devices

GPS and App Surveillance

Abusers use GPS tracking and app-based surveillance to monitor victims' movements and activities covertly.

Digital and Economic Abuse

Perpetrators restrict financial access and send threatening messages to exert control digitally and economically.

Doxing

Maliciously gathering, revealing, and publishing someone’s private or identifying information online without their consent, usually with the intention to harass, intimidate, threaten, or harm

Medjacking and Stalkerware

Medical devices and stalkerware are exploited to hijack health equipment and covertly monitor victims.

IoT Device Manipulation

Smart home IoT devices are remotely controlled to intimidate or restrict victims in their own homes.

Nest Accounts (Smart Thermostat)

- Nest is a line of smart home products from Google. Devices you can use with your Nest account include smart speakers, thermostats, fire alarms, and more.
- If someone has access to your Nest account, they can control these devices and use them to frighten, harm or monitor you.

Top Tips For Nest:

1. If you use voice-controlled Nest devices, your account will store your voice requests by default. You can delete transcripts of voice requests and disable this feature in your Google account on the 'my activity' page.
2. Check whether Google is automatically storing your data, such as your location history. If someone were to gain access to your account, they could view this data and find out a lot of information on where you have been and what you have been doing, so consider disabling this feature. You can turn this feature off in your Google account settings.
3. When not using voice activation to interact with your Nest system, consider muting the microphone on your Nest speakers as someone with access to the device could remotely activate the microphone to listen in on your conversations. If you are concerned someone in your home might use your Nest system to monitor you because they have access to the account, consider disabling personal results. Personal results are things like calendar appointments or shopping lists. Nest devices are programmed to only recognise your voice for personalised results, but are not always fool proof.
4. Don't link Google accounts which hold sensitive information about you, such as your banking information, to your Nest system. Instead, consider creating a separate Google account just for your Nest devices.
5. Turn off your Nest devices while you are away. The Nest system doesn't have an off button, so unplug the devices you won't need while you're gone.
6. Turn off your internet connection to Nest when not in use.
7. Ensure your WiFi is strong and secure.
8. Install software updates as this ensures all the security features of the device are up-to-date and more difficult to override.

Google Home Hub

- The Google Home Hub is the virtual assistant that powers a range of smart home devices by Google, called Nest devices. The Google Home Hub that is set up in your home can be accessed remotely from a connected device such as a phone or laptop.
- This means that if someone has access to your Google Home Hub, they could monitor what you are doing in your home remotely, or even make changes to your devices to abuse you.

Top Tips For Google Home Hub

1. Your Google Home Hub account will store your voice requests you make via your smart devices by default. You can delete transcripts of voice requests and disable this feature in your Google account on the 'my activity' page.

2. Check whether Google is automatically storing your data, such as your location history. If someone were to gain access to your account, they could view this data and find out a lot of information on where you have been and what you have been doing, so consider disabling this feature. You can turn this feature off in your Google account settings.

3. When not using voice activation to interact with your Google Home Hub, consider muting the microphone on your Nest speakers as someone with access to the device could remotely activate the microphone to listen in on your conversations. If you are concerned someone in your home might use your Google Home Hub to monitor you because they have access to the account, consider disabling personal results. Personal results are things like calendar appointments or shopping lists. Nest devices are programmed to only recognise your voice for personalised results, but are not always fool proof.

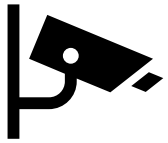
4. Don't link Google accounts which hold sensitive information about you, such as your banking information, to your Google Home Hub. Instead, consider creating a separate Google account just for your home devices.

5. Turn off your Nest devices while you are away. The Nest system doesn't have an off button, so unplug the devices you won't need while you're gone.

6. Turn off your internet connection to Nest when not in use.

7. Ensure your WiFi is strong and secure.

8. Install software updates as this ensures all the security features of the device are up-to-date and more difficult to override.



Wireless CCTV Systems

- Wireless security cameras are closed-circuit television (CCTV) cameras that transmit a video and audio signal. They can be cloud based – storing video in the manufacturer's cloud system, or network based – storing video to a user's device. The cloud-based storage system can be compromised if an untrusted person has access to it. Network based storage could also be compromised, as an untrusted person could set the CCTV up to store images on their personal device.

- This means the untrusted person would be able to see what the camera is recording and therefore monitor your home and your actions. If an abuser has access to your CCTV system, they may be able to keep a tab on what you are doing, who is coming and going from your home and use this information to control or abuse you.

Top Tips For Wireless CCTV

1. Set up two-factor verification on the associated account.

2. Check your camera's password settings. We recommend setting a strong, unique password for the device and not disabling the password settings. A strong password is long, has multiple letters, numbers and special characters, and doesn't include any personal information, or information that someone could easily guess.

3. If you can access your camera's video feed remotely, it means that your camera is sending information via the internet. It's therefore important to look for a CCTV system that encrypts your information, including your username, your password, and the live feeds and ensure the encryption feature is enabled.

4. Allow different levels of access to other users if your wireless CCTV needs to be accessed by multiple users. For example, some cameras offer separate settings for administrators, who can make changes to the settings.

5. Check regularly for software updates. Register your camera or sign-up to the manufacturer's mailing list to get updates that keep the software current and as secure as possible.

6. If you are accessing the camera from a mobile device, make sure that security features are in place for mobile access:
    - Confirm that your app is up to date
    - Protect your mobile device with a password or PIN and lock screen
    - If the app requires a separate password, use a strong password
    - Only access the app through a secure Wi-Fi connection that you trust

7. Ensure that the Wi-Fi system your CCTV is connected to is strong and secure. Continue this virtual tour to learn more about securing your wireless systems.

Video Doorbells

- Ring doorbells, like other video doorbells, are designed to allow you to see who's at the door when you're not in the property, or don't want to open the door. It's a smart doorbell that has a high-definition camera, two-way microphones and a motion sensor. The device will send a notification to the owner's phone, via the Ring Doorbell app, when someone is at the door.

- The video function means that the owner of the doorbell will be able to watch who is coming and going, and the audio function allows them to speak to whomever is at the door. This means that Ring doorbells, and other similar devices, can also be misused to monitor who is coming and going from a building.

Top Tips For Ring Doorbells

1. To ensure your Ring Doorbell is not being accessed by someone else; make sure only you have admin access to the account and only people you trust can link their devices to the Ring Doorbell. Ensure that only the administrator of the account can make changes to the Ring Doorbell settings. If you don't have admin access to the account, consider resetting the device to give you control of the admin function if that feels the safest course of action.

2. If you do have admin access to the Ring Doorbell, you could also review all other devices connected to the Ring Doorbell in the 'settings' area. Linked devices could include Smart TVs, Alexa's, phones and tablets. Someone may be able to gain access to the doorbell through these devices, so it is important to know what the Ring Doorbell is connected to and remove untrusted devices if it's safe to do so.

3. Consider enabling two-factor authentication via the Ring Doorbell app, to give you additional protection and in so doing ensure other people can't add their own accounts to the Ring Doorbell. Other smart doorbells will also have this feature.

4. Review shared users on your Ring Doorbell app often to check whether any unknown users are linked; this can be done through the app connected to the device and by going to 'settings'.

5. Ensure your WiFi is strong and secure.

 Smart Locks

- A smart lock's basic function is to allow you to lock and unlock your door via an app. They can monitor access to your home and send notifications to the owner of the smart lock about when people arrive at and leave the home. You can also lock people in or out remotely.

- If compromised by someone else without your agreement they can be used to see, track and monitor what you are doing.

Top Tips For Smart Locks

1. Check who “owns” the account on the smart lock app on your phone. If it is not you, or you only have a guest account, consider resetting the lock completely.
2. Check whether the account or system you use to access the smart lock has a strong password.
3. Make sure the phone you use to access the smart lock is also secure (use a passcode; ensure no-one else has access to the Apple or Google account that backs up your phone’s data).
4. Check whether the door on which the smart lock is installed is strong and secure, as the smart lock could be by-passed with brute force.
5. If the lock supports “Guest Access” check who has guest access. If there are any people, accounts, or devices you don’t recognise consider removing them if this feels safe. You may also want to consider resetting the lock.
6. If the lock supports key cards, PINs or fingerprints -- you may want to disable all of these or change the PINs if other individuals have had access to your smart lock previously.
7. Install and check for updates to the hardware and software regularly.
8. Ensure your WiFi is strong and secure.

Fitness Trackers & Wearables

Apple Watch

- The Apple Watch is a smart watch designed by Apple. It can connect to all your other Apple products when you set up using your Apple ID. It can be used as a fitness tracker and for calls and messages when you don't have your mobile phone to hand, and through which you can access Apple's virtual assistant, Siri.

- It has access to your location, messages, call logs, calendar and other information which can be used to monitor and track you if someone has access to your Apple ID.

Top Tips For Apple Watch

1. Set a strong passcode lock to prevent others gaining access to your watch.

2. Ensure your Apple ID account is secure. You can view all devices linked to your Apple account from your Apple device. If there are devices listed that are not yours, or you don't recognise them, you can remove them. This may alert the person using the devices connected to the account so if that might put you at risk, consider seeking further help.

3. Make use of the activation lock, especially if you do not own any other Apple products. This is designed to help you if your watch is lost or stolen. If someone tries to un-pair or tamper with your watch, they will be unable to do so without your activation lock.

4. If you already have other Apple products and use the 'find my' function, you will be able to view your Apple Watch in 'find my'. Should the watch become lost or stolen, you will be able to remotely secure the data your watch holds from another device or desktop.

5. Consider turning on wrist detection for your Apple Watch. This means that when the watch detects that you are not wearing it, the watch will automatically lock to keep your data secure.

6. Consider turning on the erase data function. This erases all data from the device after 10 unsuccessful log-in attempts, protecting you if your watch is lost or stolen.

7. Consider enabling notification privacy. When you receive a notification, such as a message, the content of it won't be openly displayed until you enter your passcode. Make sure your device is regularly updated to ensure that you have the most up to date security features in place.

Amazon Alexa and Amazon Echo

- Alexa is a virtual assistant available on several Amazon smart home products. Alexa is capable of voice interaction, playing music, adding items to your shopping lists and more. Alexa controls Amazon Echo devices. Echo devices can come as a speaker or a device with a screen and a camera (such as the Echo Show) and are often linked to 3rd party services, such as Spotify or Audible accounts.

- This tech can also be misused to monitor what happens in your home as someone with admin access is able to listen to the audio picked up by the device's microphone or view your home via the video features without you ever knowing. If another person has access to the device, they are also able to command the device to do things such as play music or send voice messages without consent.

Top Tips For Amazon Echo

1. For your privacy, you can disable the mic by pressing the Echo's top 'Mute' button when it isn't in use. If you're using an Echo Show you can disable the mic using the slider button. You'll still be able to use the Echo using your Alexa Voice Remote – all you have done is disabled the microphone itself.
2. Switch the Echo's sound notification on to automatically alert you if your Echo is accidentally triggered, meaning it is recording audio.
3. Disable your smartphone's address book sharing feature, as someone with access to the Amazon device could use it to call or message people in your address book.
4. Amazon automatically stores all your Echo's interactions to improve its performance and command accuracy. For extra privacy, regularly review and delete your activity through your Amazon account or opt out of recordings all together.
5. Consider turning your Amazon Echo Show's camera off.
6. Use PIN protection or disable voice purchases to stop someone making unauthorised voice purchases.
7. Install software updates as this ensures all the security features of the device are up-to-date and more difficult to override.
8. Read third-party terms and conditions to understand what other apps your device pairs with and what apps may have access to the device.
9. Make sure your WiFi is secure to prevent visitors or others who have been on your network previously from accessing your Echo and Alexa devices. Continue this virtual tour to learn more about how to best secure your wireless systems.

Smart TVs

- Smart TVs offer the user all the functions of a standard TV with added extras, installed from an app store. You can often install 3rd party apps like Netflix, Skype, or browse the internet. Smart TVs often (but not always) have built in mics and cameras.

- When Smart TVs have mics or cameras, they can be misused to monitor people in the home. When someone has access to your Smart TV they can also make changes on it that could be confusing or intimidating.

Top Tips For Smart TV

1. Check that the accounts you're accessing through the TV are secure. This means checking whether the email linked to your Smart TV is one you have access to; checking that untrusted people don't have access to the accounts linked to the TV and that no-one knows or could guess the passwords for your linked accounts.

2. Review your TV's privacy settings – it's easy to automatically 'agree' to the suggested privacy settings when setting up the TV, but you may want to consider what data the device has access to. It's not advisable to agree to your data being collected.

3. It's advisable not to share the login details for the main account for the TV as these could be used to make changes to the TV or to activate the cameras or microphones on the TV. Always follow strict sign-in criteria to keep your TV's user accounts and in-app profiles safe and secure.

4. Avoid inputting financial information into your TV's apps.

5. Consider creating secondary user profiles, which have their own sign-in information and user restrictions.

6. Ensure you update your TV's software, hardware and app software regularly as this ensures all the security features of the device are up-to-date and more difficult to override. The procedure for installing system updates on your TV varies depending on the model and manufacturer, so consult your user guide if you need more details. If you're given the option, make sure auto-update options are turned on.

7. Use an antivirus for your smart TV as it can be infected with malware or viruses just like your other smart devices.

8. Consider covering your camera when you're not using it. Some TVs link to other smart devices, such as phones and tablets. If someone has access to the TV account, they could activate the camera to broadcast an image of the room, without you knowing.

9. Consider disabling your TV's microphone when you're not using it as it could also be activated remotely, allowing someone to listen in on your conversations.

Smart plugs

- Smart plugs sit in your electrical outlet and connect to your smart home system. They allow devices that are not smart-enabled to ‘become smart’ and be controlled using your smart home system, for example a lamp. The lamp, and other items, can be activated through an app or voice commands.

- Smart plugs can be misused by someone turning on appliances in your home remotely to scare or harm you.

Top Tips For Smart Plugs

1. When setting up your smart plug, check you're using a wall socket that is not overloaded with extension leads, and is clear of furniture to reduce risk of fire.
2. Before installing, check whether the account linked to your smart home devices is secure (this could be your Amazon account if using Alexa enabled products or your Google account).
3. Ensure your wireless network is secured with strong passwords and consider reviewing the devices that have access to your wireless network. Continue this virtual tour to learn more how to best secure your wireless systems.
4. Regularly check for and install software updates for your device, this will ensure it has all the latest security updates.

Wireless system

- Wireless systems are a collection of devices that interact with each other without the use of cables. They often use your WiFi to work. Examples of wireless systems might include home devices like wireless smart speakers, or home security cameras.

- Ensuring that your WiFi is secure is one of the key steps to protecting your wireless systems because an insecure WiFi can give someone access to all the devices connected to your wireless system.

Top Tips For wireless system

1. It's important to secure your passwords for your router, your WiFi Admin, and the accounts linked to your wireless devices. Never use the password set by your internet provider and make sure you set a strong and unique password that is difficult to guess.
2. Consider setting up a guest WiFi account for visitors to use to avoid you ever having to share your WiFi codes.
3. Consider purchasing wireless systems with encrypted signals. This means that only authorised devices will be able to communicate with your wireless system. For the best security use WPA3 encryption. If it is not available, use WPA2. Do not use WPA or WEP.
4. It's advisable to install antivirus software to detect virus or malware threats which will alert you if your device is compromised by malware that could be used to spy on you. Limit devices that can interact with your wireless systems to only the devices you own.
5. Install software updates as this ensures all the security features of the device are up-to-date and more difficult to override.
6. Consider disabling the "Remote Management" feature as it can be abused.
7. It is strongly encouraged to disable features like UPnP, port-forwarding or remote management, which could open the door to the attackers.

Smartphones & Tablets

Surveillance and Monitoring

- **GPS Tracking**: Perpetrators install apps or use built-in location services to track victims' movements in real time.
- **Access to Accounts**: Abusers demand passwords or install spyware to monitor emails, social media, messaging apps, Strava, Uber.

Stalkerware and Spyware

- Stalkerware (also: spyware, spouseware) refers to software installed on a device without the user's knowledge or consent, enabling covert surveillance
- Apps disguised as parental controls or security tools allow covert monitoring of calls, texts, browsing history, and even keystrokes.
- These apps often run silently, making detection difficult for victims.

Harassment and Threats

- Persistent, obscene, or threatening messages sent via SMS, WhatsApp, or social media.
- Victims may receive hundreds of messages daily, creating psychological pressure and fear.

Economic Control

- Mobile banking apps are exploited to restrict access to funds, monitor spending, or make unauthorized transactions.
- Victims can be locked out of financial accounts, deepening dependency.

Remote Access and Device Control

- Perpetrators use cloud accounts (e.g., Apple ID, Google) to access photos, messages, and location data.
- They may remotely wipe devices or lock victims out, causing distress and loss of evidence.

Evidence Gathering for Coercion

- Screenshots, recordings, and stored messages are used to blackmail victims or threaten exposure of private information

🎥 Baby (Pet) Monitors & Cameras

- Baby monitors and cameras can be misused by perpetrators to monitor victims' movements and invade their privacy. These devices often allow remote access through apps or cloud accounts, enabling surveillance even when the abuser is not physically present. In some cases, abusers manipulate the devices by changing camera angles or activating audio features to intimidate victims and reinforce control.

- Recordings captured through these devices can also be used for blackmail or threats, increasing psychological pressure. Victims may notice signs such as cameras being repositioned, unfamiliar devices connected to the monitor, or unusual activity like unexpected sounds or alerts.

AI/ Deep Fakes

- Government data shows deepfakes have exploded from 500,000 in 2023 to 8,000,000 in 2025 - Government leads global fight against deepfake threats - GOV.UK

- Deepfakes and AI technologies are increasingly being weaponized by perpetrators of abuse to harm and control victims. These tools allow abusers to create highly realistic fake images, videos, or audio recordings, often without the victim's consent. Such content is frequently sexualized or humiliating and can be used for blackmail, coercion, or reputational damage.

- Because deepfakes are difficult to distinguish from authentic media, victims face significant challenges in disproving fabricated material, which amplifies psychological distress and fear of exposure.

💉 Medical Devices

- Tech Abuse can also extend into the healthcare domain. In documented cases, Bluetooth-connected medical devices (e.g. insulin pumps) have been hijacked in attempts to cause harm—what has been dubbed “medjacking”.

- The NHS App has been misused by perpetrators of domestic abuse as a tool for control and surveillance. Because the app provides access to sensitive health information, appointment details, and sometimes location data linked to healthcare visits, abusers can exploit it to monitor victims’ medical records and activity.

- In some cases, perpetrators have coerced victims into sharing login credentials or installed the app on shared devices, enabling them to track prescriptions, mental health appointments, or even pregnancy-related care.

Smart Cars

- Smart cars enable tracking primarily through their built-in connectivity and location services. Modern vehicles often come equipped with GPS systems, telematics, and apps that allow remote access to the car's data.

- These features can be misused by perpetrators to monitor a victim's movements in real time. For example, linked accounts or companion apps (such as those provided by manufacturers) can show the car's current location, route history, and even geofencing alerts when the vehicle enters or leaves certain areas.

- Additionally, smart cars often sync with smartphones, storing location data and trip logs that can be accessed remotely if the perpetrator has login credentials. Some systems allow remote control of functions like locking, unlocking, or starting the car, which can be used to intimidate or restrict a victim's mobility

Checklist: Identifying Technology-Facilitated Abuse Risks

This checklist helps identify potential technology-facilitated abuse risks:

Communication Monitoring

Unexplained access / knowledge of victim's messages, emails & locations or victim reports partner reading private conversations

- **Questions to ask**: Has anyone demanded your passwords or installed apps on your phone? Does anyone else have access to your passwords? Were you gifted your phone?

Location Tracking

Victim feels constantly followed or located or Presence of tracking apps or Air Tags

- **Questions to ask:** Do you notice alerts about location sharing or unknown devices? Are there accounts/ apps that you partner/ ex-partner could have access to? Could anyone else have access to your Wi-Fi, smart devices or car devices?

Financial Control

Restricted access to online banking or payment apps or unusual transactions or locked accounts.

- **Questions to ask:** Has anyone blocked or monitored your financial accounts?

IoT Device Misuse

Smart home devices controlled remotely without consent or unexpected changes in heating, lighting, or locks

- **Questions to ask:** Are household devices behaving strangely or controlled by someone else?

Stalkerware/Spyware

Phone battery drains quickly or unknown apps installed or victim suspects covert monitoring

- **Questions to ask:** Have you noticed apps you didn't install? Are there unrecognized apps shown on your battery usage page?


TECHNOLOGY
MINIMISING DENYING OR BLAMING
Stating that restrictions and tracking software are for your safety
Blaming tech problems and computer virus on you
USING OTHERS
Getting other people to post abusive or threatening messages on social media
Doxing – sharing account details without consent or knowledge
ECONOMIC ABUSE
Tracking or accessing bank accounts or financial records
Using identity theft to apply for loans and credit cards
Denying access to online bank accounts
Online activities that damage credit rating
Monitoring purchases
USING PRIVILEGE AND OPPRESSION
Forced surrender of login details
Making all the decisions about the use of technology
Locking out of devices by changing passwords
Determining when and how technology is used
COERCION AND THREATS
Using emails, texts and social media to make threats
Posting false information
Threatening to images on social media
Threatening to break devices
EMOTIONAL ABUSE
Degrading or embarrassing someone online
Causing confusion by changing settings remotely, or deleting items
Online grooming
ISOLATION
Restricting access to wifi and smart devices
Closing accounts to end relationships with others
Replying to messages with others
Infecting computer with viruses to erase data and prevent usage
INTIMIDATING MONITORING AND STALKING
Changing passwords to accounts without consent or knowledge
Constantly making contact via text or social media
Monitoring contacts, texts, social media activity or internet activity
Using devices to track or
Recording conversations
Using fake accounts and identity theft
POWER AND CONTROL
TECHNOLOGY
Allison Baden-Clay Foundation
allisonbadenclayfoundation.org.au

Summary

Examples of Tech Abuse

- Tracking movements via GPS or apps
- Economic abuse through banking apps
- Hijacking medical devices (Medjacking)
- Misusing IoT devices (smart locks, cameras, voice assistants)

Impact

- Tech Abuse intensifies coercive control, creates persistent surveillance, and can cause financial, psychological, emotional, and physical harm.

Recommendations

- Ask direct questions about tech abuse and how a person is being monitored, controlled & abused.
- Use safety planning and focus on keeping safe online, awareness of apps and smart technology.
- Promote ‘digital consent’ education with service users.