Keeping Safe from Technological Abuse

What is Technological Abuse?

Technological abuse is the use of any technology to gain power or control. There are four main ways it is used:

1. Disrupting your use of technology either by forbidding its use or changing your password to stop you accessing it
2. Setting up accounts in your name on porn sites, dating sites or even social media which they can then use to harass you, your family or friends
3. Repeatedly harassing you by text, messaging apps such as WhatsApp and Viber or email
4. Monitoring and tracking your physical and online behaviour

To keep safe, consider your whole digital footprint, and what you need to know to be more secure and less visible.

Get to know your Mobile Phone

- Make sure you have the latest operating system on your phone.
- Put a reminder in your diary every 6 to 9 months to make sure you are keeping it up to date
- You can the user manual for your phone by searching online for the manual. For iPhones more information is available here: iPhone Privacy & Security
- Protect your device with a PIN, keep it secret, and change it regularly
- Do not use biometric (e.g. thumbprint) to secure your phone as your abuser take your thumbprint (for example) while you sleep to open your phone
- If you can't secure your phone, consider using a prepaid SIM for secure calls and messages, and keep it safe.

Use Secure Passwords

- Use a combination of letters, numbers and symbols when creating passwords
- Consider replacing letters with numbers in words e.g.H3llo not Hello
- Use a passphrase e.g.: ice-limp-chill
- Use different passwords for every site you sign up to
- Do not let your browser save your password, especially if you share devises with your abuser
- Consider using a secure Password Manager – you can read more about it here: Password Managers
- Where you can use Two-Factor Authentication , it makes it t harder for anyone attempting to hack your accounts. Sites that allow that can be found here: Two Factor Authentication

Keep your Chat Conversations Safe

- Always use a trusted device
- Use encrypted messaging services such as What'sApp and Viber
- Be aware that phone numbers you call can be seen on your phone bill, especially if your abuser has access to this.
- If you are unsure if your device is secure, use a prepaid SIM card and keep it safe

Keep your Location Safe

- Check which apps are using your location and, if you don't need it, withdraw permission. More information on how to do that can be found here for iPhone and Android
- Don't allow messaging apps such as What'sApp and Viber to show your location. Find more information here for WhatsApp and Viber
- Some apps, such as Google Maps, won't work unless you share your location. Consider only allowing it when you need the application.

Be Mindful of Tracking Software

Tracking software may have been added to your phone if it:

- The batter runs down faster than it should
- It says lit when you try to turn your screen off
- Runs slower than normal
- Find unfamiliar applications running in the background
- Takes forever to shutdown

Other signs may be:

- Your abuser knows where you've been or the content of an email or who you've spoken to
- You receive notifications that someone has been accessing your account. Don't ignore these. Change your passwords immediately.
- Antivirus software can be helpful in identifying software that's been installed without your knowledge. Find out more here: AntiVirus Software for Mobiles

If you think someone may have installed tracking software, return your phone to factory settings, and reset it with a strong password. Do not use biotech features, such as thumbprint.

Keeping Safe with Social Media

- Make sure you use two factor authentication for social media accounts, and use a secure email
- Do not allow your social media to show your location
- Set your account private or use a fake user name
- Block or 'unfriend' your abuser
- Be mindful of mutual friends and ask them not to post to your page or tag you on social media as your abuser could see these
- Be careful that any photos your post do not give your location way by showing where you are e.g.: the street name, or an identifiable buiding.
- Twitter Safety Guide
- Keeping Safe on Facebook
- Keeping Safe on Instagram
- SnapChat Safety Guide
- TikTok Safety Guide

Keep your Email Conversations Safe

- Gmail allows you to review when and where your email has been accessed. You can find out how here: Check your Gmail Login History
- Remember that sent items are stored in your 'sent' folder, unfinished emails in your 'draft' folder and deleted emails in your 'deleted' folder. To permanently delete deleted emails go to the folder and select the option to delete it.
- Don't click on suspicious links in emails or texts, even if it looks like the email has come from someone you know.
- Only use secure public computers. At hotels, for example, are accessible by other people who can put keyloggers or other malware on them. Wait to do your online banking or access other highly personal accounts on your secure device

Keeping Safe when Online

- If you use multiple devices, make sure you shut down applications when you have finished using them. Do not keep signed in on a device you are not using.
- If you have joint accounts for things such as iTunes, App stores, Google Play store, eBay, Amazon, Kindle , Spotify, and others either stop giving your abuser access, or create a new separate account. Your abuser could use it to stalk you or leave unwanted messages, for example, by adding songs to your spotify list that have special meaning to you both.
- Be especially vigilant when researching travel plans, housing options, legal issues, safety plans or other similar information. Use a safe computer e.g. at your library
- Get in the habit of deleting your browers history, cookies and cache when you sign out. More information can be found here: Deleting your Browser History.
- Major browsers such as Chrome, Firefox, Internet Explorer and Safari enable you to browse privately by using their ' incognito' mode. This means that no traces of your activity will be left on your computer, such as the history of sites that you have visited. This option can be found under the menu or tools options. Detailed advice on browsing privately can be found via the help option of your browser.
- If you're unsure what browsers you're using, you can check here: Check Your Browser
- More information on keeping safe on line can be found here: Cover Your Tracks Online

Be Camera Aware

- Cameras and devices can be accessed remotely or activated by apps.
- Cover the webcam on your computer/tablet when not in use. You can find webcam covers on Amazon and other tech sites.
- If technology has been given to your children, such as gaming, make sure those are covered too

Be Aware of Spyware

- Spyware is a computer software program or hardware device that enables an unauthorisd person (such as an abuser) to secretly monitor and gather information about your computer use.
- It can be installed remotely or in person. It works by tracking every keystroke your type, application you use, website you visit, every document you open, everything you print.
- Some spyware software gives the person monitoring the ability to freeze, shutdown or restart your computer. Some versions even allow the abuser to remotely turn on your webcam or make your computer talk.
- It can run in stealth mode, and be difficult to detect
- If you think spyware may have been installed, replace your device or computer
- More information can be found here:
    - Malware Bytes – What is Spyware?
    - Which? Free and Paid Antivirus Software
    - Technology Safety
- More information on how you can tell if there are hidden cameras in your home can be found here: How to Detect a Nanny Cam

What to do if intimate photos of you have been posted online

You can check if intimate photos of you have been posted online by searching for your name on Google . You can also search by image. Go to Google Images , and click on the camera icon in the search bar. If you find an nude or private photo in the search results document by taking screenshots of the full web page, where its posted and the search image.You can then report them to google by filling out this form.

Some websites, such as Pornhub, have dedicated content removal forms in order to tackle revenge porn. If you found your images on Pornhub, you can fill out their form here.

If inappropriate images of you are posted on social media , you can ask for it to be removed here: Remove Images from Facebook, Remove Exposed Private Information on Twitter, Report Abuse on Snapchat

If you need help you can contact the Revenge Porn Helpline

Store Files Securely

- Save files to an encrypted online storage service, e.g,: dropbox
- Use two factor authentication to help prevent anyone else accessing your data
- If you are asked to enter a backup email address or a second phone number, consider supplying the email or phone number of a trusted friend rather than one of your own.
- Use USB Sticks with secret partitions. If your abuser were to get hold of one of these partitioned USB sticks and plug it into a computer, the USB stick would appear to be broken rather than revealing all of your files.
- Scan your most important records (e.g. birth certificate, immigration papers). These records will make it easier for you to get these documents back in case your abuser takes them away from you.
- If you don't have access to a scanner or photocopier, head to your local library
- Note : some experts advise against online storage of files, but it is safer than keeping them on your personal devise if your abuser has access to it

Keep Safe when Gaming

- You don't know who you are talking to when gaming. Use a username that doesn't identify yourself, and don't' give any identifying information away.
- Use different email address, user name and profile picture for each game you play, and make sure its different to your social media accounts. This stops someone being able to connect your gaming profile to you in real life.
- Be careful about attachments and links that are sent to you via a game, which might install spyware or other malware on your devices.
- Be mindful on your child's online gaming activity. If online games have been given to your children, your abuser may be communicating with them outside of contact hours or using the game to spy on you.

Be Safe in your Car

- GPS trackers can be attached to your vehicle and can be difficult to track
- Be aware that if your abuser knows your vehicle (model, licence plate) it makes it easier for them to find you
- If you suspect a GPS tracker, consider asking a trusted friend to give you a lift or use a taxi or public transport. Where you can, pay with cash.
- Be careful with ride-sharing apps, because they may make your detailed ride history available through the app and leave evidence on your credit card statement.

Be Safe at Home

- Keep your wifi secure with a strong password. Make sure only you know it.
- If someone can access your wifi they can use it to track your online activity
- Be aware of smart home devices e.g. Amazon Echo (Alexa), Google Home, a smart thermostat, house alarm system or other controls that can be accessed remotely and could be used to monitor you or to harass or isolate you, without your knowledge.
    - This could include thermostats, Smart lightbulbs, Smart electrical outlets (with lights or other devices plugged into them), Entertainment systems (stereo, TV, etc.), Hubs that are located on a bedside table, or other locations throughout the house that connect to the home personal assistant, Security cameras and motion detectors, Smoke detectors, Video doorbells, Smart locks, Appliances (refrigerator, vacuum, etc.), Pet feeders, nanny or pet cams, toys and trackers, Children's toys and trackers This is especially true if they come with features that can be abused such as camera, microphones or motion centres
- Think about what you need and get rid of anything you don't use or are not sure about
- Change the passwords on the ones you keep to a secure password, and do not give it to anyone else

Document Any Technological Abuse

- Documenting is important to:
    - Help you narrow down what's happening
    - Alerts you to any escalation in behaviour
    - Gives you proof if you want to pursue legal action
    - Keep a log of all incidents, even if you are not sure if you want to involve the police.
- Details of what to document can be found here: Documenting Technology Abuse

If you need help:

- For queries regarding counselling call the Woman's Trust on 020 7034 0303
- If you are in immediate danger call 999
- For 24/7 advise on domestic abuse call the National Domestic Abuse Helpline on 0808 2000 247

References:

Avast.com
Bedfordshire Domestic Abuse Partnership
The Defence Works
Express VPN Tech Safety Guide
GadgetSpy
Get Safe Online
How to Geek
Living Without Abuse
Malware Bytes
Reducing the Risk.Org
Refuge – Tech Abuse
Royal College Nurses – Keeping Safe Online
Safelives.Org.UK
Tech Radar
TechSafety.org
UK PC Mag
Which?
Women's Aid – Online Safety
Women's Media Centre

Be alert,
Trust your instincts,
Do what you need to do to
Feel Safe and
Stay Safe.