Technology Facilitated Abuse

7-minute briefing

What is Technology Facilitated Abuse? 1

Technology facilitated abuse is the use of technology to enable any form of abuse. This could include:

- Monitoring calls, texts and location
- Harassment, intimidation and stalking
- Coercive and controlling behaviour
- Financial abuse
- Many other forms of abuse

This could occur via:

- Direct physical access to a device
- Remote access through known account passwords etc
- Remote access through sending and accessing malicious links
- Stalkerware / spyware / tracking devices

Device security 2

To prevent unauthorised access to a device use:

- ❑ Strong passcodes (not anything personal that could be guessed)
- ❑ Fingerprint or face ID (biometrics)
- ❑ Turn off location tracking and review your sharing settings to prevent your data being shared with / seen by others
- ❑ Update your emergency / SOS contact
- ❑ Check your apps for anything unfamiliar or causing unusual battery drain and remove them
- ❑ Keep antivirus software updated

Phone calls and video 3

To protect the security of your phone and video calls:

- ❑ Secure voicemail with a strong PIN
- ❑ Use private links and secure waiting rooms to control who joins video calls
- ❑ Review your background in video calls and photos to make sure there is nothing giving away your location or data
- ❑ Cover webcams when not in use
- ❑ Use mobile data instead of wi-fi to prevent IP tracing

Online presence 4

Upgrade the security of your online presence by:

- ❑ Control who sees your social media posts – regularly review security settings
- ❑ Review friends / follower lists regularly and remove anyone you don't personally know
- ❑ Be aware of what is in the photos you are sharing and if someone could use it to find your location (e.g. distinctive buildings / street signs etc)
- ❑ Be aware of what others are sharing about you
- ❑ Use private browsing and delete browsing history
- ❑ Use account recovery tools if needed and sign out of devices/accounts when finished

Smart tech, vehicles and location tracking 5

Keep your smart tech safe:

- ❑ Change your home wi-fi router name and password from the factory set ones
- ❑ Disable remote access to your router
- ❑ Clear your SatNav or vehicle navigation history
- ❑ Review vehicle / smart tech app access and regularly review and update credentials and passwords
- ❑ Be aware of physical tracking devices such as AirTags

Password hygiene & account protection 6

Keep your accounts protected:

- ❑ Use strong unique passwords (e.g. three random words)
- ❑ Avoid reusing passwords or using passwords that are predictable or easy to guess
- ❑ Email passwords need to be extra strong
- ❑ Have a separate email account just for email/ device recovery that is known to nobody but you
- ❑ Choose security questions that are not easily guessed (beware of social media questionnaires asking for information that may be used to guess theses answers)
- ❑ Use two-factor authentication (2FA)

Key takeaways 7

- Use strong passwords, biometrics and 2FA
- Be aware of what you are sharing online and who can see it
- Clear your history
- Run all software updates and update your antivirus
- If in doubt – seek help!

Support

Help is available

National Cyber Security Centre: Top tips for staying secure online

Refuge: Information and support on tech abuse | Refuge Tech Safety

NIDAS provides support to victims of domestic abuse in Norfolk: Home – NIDAS

Norfolk & Suffolk Victim Care provide support to all victims of crime

NORFOLK COMMUNITY SAFETY PARTNERSHIP