

Technology is changing the world and whilst technology can help keep people safe, abusers can also exploit technology to cause harm.

Technology can enable and empower Domestic Abusers; they can bombard their victims with calls and messages while limiting their contact with friends and family. They can also share, or threaten to share, private, sensitive or intimate information online. Tech abuse is hard to spot and hard to escape. But if you know the risks you can take steps to keep yourself and others safe.

The growing risk of tech abuse (extracted from UCL guidance)

The Internet of Things (IoT) is a term used to refer to 'smart' Internet-connected devices that can share data with each other, creating a 'network' of devices. Going beyond laptops, phones and tablets, IoT includes smart watches, and internet-enabled household appliances such as smart fridges, TVs and locks. Studies estimate that by 2030 there will be 125 billions devices connected to the internet.

IoT devices are 'smart' because of how they collect and send data, analyse this data, and take action, potentially without direct human intervention. When IoT devices are connected to the Internet they can communicate and share instructions with each other. This can result in privacy, security, and safety risks, because devices assume all users trust each other. An abuser can potentially misuse IoT devices' features to monitor and control a victim.

IoT devices and possible risks

- **Wearable devices – such as smart watches** - could enable abusers to track and monitor movements and other behavioural patterns drawing on GPS signals and other collected data.
- **Phones** - could provide abusers with an access point to control various IoT devices.
- **Laptops and tablets** - accounts between devices are linked and could allow abusers to change and review IoT devices' settings via an Internet browser.
- **Remote control of heating, lighting and blinds** - could be used to coerce and intimidate victims by switching systems on or off from afar.
- **Audio recording** - could facilitate remote monitoring and stalking.
- **Voice control** - may enable perpetrators to contact the victim as well as trace and review a person's history of commands and purchases.
- **Router** - connects all smart home devices to the Internet.
- **Security cameras and TVs** - could facilitate remote monitoring and online stalking; video recording could facilitate image-based abuse (such as revenge porn).
- **Smart security** - could provide access to doors through voice activation, apps, or electronic key codes.

Helpful Resources

- [Refuge](#) has published resources to support people at risk of tech-abuse.
- [UCL](#) have illustrated how smart devices present new risks for victims of domestic violence & abuse.
- [Safe Lives](#) have produced a guide for practitioners to support them to have conversations with adults at risk about using technology safely.
- Ann Craft Trust have produced an [introduction to digital safeguarding guide](#) which explains what digital safeguarding is and provides tips and advice for staying safe online.
- AVA, CAST and Comic Relief collaborated on a comprehensive [Digital Safeguarding Resources Pack](#).

Abusers can use technology to maintain control.

They can bombard their victims with calls and messages while limiting their contact with friends and family.

They can also share, or threaten to share, private, sensitive or intimate information online.

#SafeguardingAdultsWeek

ann craft trust
acting against abuse

Thank you for taking the time to read this Learning Brief. If you would like to provide any feedback or have any questions regarding the Board, please contact: Lynne.Mason@Reading.gov.uk