Internet of Things/Smart devices

Items which are part of the 'internet of things', or smart devices, encompass a wide range of internet-connected and enabled devices, from doorbells to washing machines. Unfortunately some of these devices can be used to stalk or eavesdrop on a victim of abuse, or carry out harassment. Poorly protected smart devices can also offer a relatively easy way to hack home networks - this does still require some level of technical skill from the abuser.

For any smart device that has been previously been controlled by an abuser who no longer has access to the home:

- Factory reset the device, setting it up from scratch with your own account
- Apply strong separate passwords to smart device accounts
- If it's not essential that the device be online, considering disconnecting it

Video doorbells

These doorbells are useful for home security, and interacting with callers when away from home. They can:

- Record when the doorbell is pressed as well as any interactions with callers
- Activate recording and send a notification when someone approaches the door
- Allow residents of the home to respond to the front door remotely
- Work after dark, using night vision recording and motion sensors

In domestic abuse cases, abusers can use a video doorbell to spy on their victim as they come and go from their home or as they have visitors.

If the victim is still in the relationship, they will have to be aware that the doorbell is monitoring the door, and that their abuser will know who arrives at and leaves the house, and when.

When a victim leaves the relationship a video doorbell is a useful piece of home security as it will allow them to know who is approaching their home. If the doorbell was originally set up by the abuser they should perform a factory reset, set up a new account, change all the passwords and apply 2-step verification (2SV), also known as two-factor authentication (2FA), where possible.

Internet-enabled cameras

Internet-enabled cameras can be used both inside and outside the home, to help secure the home or keep an eye on pets, children, or other vulnerable relatives. They can record locally to an internal hard drive or SD card, or remotely to the cloud (this is usually a subscription service).

Anything connected to the internet has the potential risk of being compromised, but cameras can be particularly alarming as they could allow someone to see inside your home. As with video doorbells, in some cases a victim of domestic abuse will be aware that cameras are there, and needs to be aware that their activity can be monitored.

Cameras can be live streamed to a mobile device and can be accessed and observed from any location 24/7. They can be switched on remotely – both camera and microphone. Some will have a light showing that they are recording/streaming, but not all do – and some that do can be switched off.

An abuser who has installed a camera will almost certainly have sole control of it, so a victim can only hope to be aware that they are being filmed. When a victim leaves the relationship, they should remove or take control of any cameras the abuser installed. If the victim can take control of a camera, they should perform a factory reset, set up a new account, change all the passwords and apply 2SV/2FA where possible.

Accounts that have been set up with 2SV/2FA require the user to provide a second factor, which is something that only the user can access. The second factor can include:

- PIN codes or a string of characters, often sent to the user via SMS or email
- a security token that the user must physically connect to their device (such as via USB)
- biometric details (such as a fingerprint scan, or facial recognition)
- an Authenticator app such as those provided by Microsoft or Google

Cameras may also be been hidden in the home without the victim realising. It may be possible to spot them connected to the router, however:

- legitimately connected devices may appear as only a MAC address, making it difficult to tell known and hidden devices apart
- cameras using mobile data will not appear

If the victim remains in the home once the abuser has left they can search physically for hidden cameras. While commercial smart cameras (for example Nest, Ring, Blink etc) are fairly large and therefore noticeable, much smaller cameras are sold for covert surveillance.

Smart door locks

Smart locks allow a homeowner to access their home without the need of a traditional key. Using Bluetooth or Wi-Fi, access can be granted using a smartphone, fingerprint, fob, fob card or a keycode. Bluetooth will allow the user to open/close the door if they are within a certain proximity; whereas Wi-Fi will enable the user to access from anywhere – including when they are away from home.

Smart locks generally do not record video, but they do send alerts, logging the opening and closing of the door.

In domestic abuse situations, a smart lock could be used by abusers to:

- Control their victim by monitoring the opening and closing of the door, to see how long they are away from the home
- Record how long the door is open for, possibly highlighting they are speaking to someone at the door
- Lock the victim in or out (e.g. by changing the access code)

While in the relationship, a victim of domestic abuse is unlikely to be given access allowing them to do anything more than lock and unlock the door.

Once the victim has left the relationship, if they keep the smart lock system, they should factory reset the system, and set up a new account with a strong, separate password. If the smart lock uses a PIN they should set it to something new that the abuser will not guess. If they cannot take control of the lock in this way, they should consider changing to a standard key lock (or a new smart lock, if finances allow).

Home hubs/smart speakers

The best known devices of this type are the Amazon Echo family ('Alexa') but there are numerous other models available.

Any requests made to a home hub/smart speaker are sent via the hub/speaker to its paired device(s) and cloud account, and recorded in both text and audio format. The app and paired account can be shared across different devices. Victims should be aware that any requests made to the hub/speaker can be seen by the abuser, if they have access to the app and account. While the victim is still in the relationship they may not have access to the hub/speaker account. If they have left the relationship, and still have the hub/speaker in the home, they should factory reset the device and set up a new account, using a strong separate password, and 2SV/2FA where available. More information on resetting devices can be found in the second-hand devices handout.

Smart thermostats/lighting hubs

Smart thermostats (e.g. Nest, Hive) control heating (and possibly hot water) in the home, while lighting hubs (e.g. Philips Hue) control lights. Smart lighting can also take the form of individual smart bulbs, which do not need a hub, or smart plugs that can control plugged-in lights.

Basic functions of these devices can usually be used by anyone in the home - e.g. changing heating settings, turning lights on and off. However admin functions and remote access will be via an app which the victim is unlikely to be given access to. This gives the abuser the ability to harass and punish the victim remotely, for example making the home too hot or cold or turning the lights on or off. This would be considered as coercive and controlling behaviour in law.

If the abuser leaves the home, the victim needs to take control of their home devices where possible. Performing a factory reset on the system will remove any existing accounts, and prompt for a new one to be set up. Victims can do this and add strong passwords and 2SV/2FA.

Other internet-enabled devices.

There are numerous household items that can be considered under the umbrella of IOT - kettles, fridges, cookers, TVs, etc.

If the abuser has left the home and the victim still has these devices connected, they should change all device passwords, including the router password and its admin access. This will prevent the abuser being easily able to access the devices or network.

Some devices may work perfectly well without internet access, and it may be easiest to disconnect them. However if they are ever reconnected, the user should check for updates to ensure they are secure.

Keeping the abuser out of internet-enabled devices means they cannot use them to harass the victim, and they cannot use them as an entry point into the home network (this is already quite unlikely, as it requires significant technical knowledge).

Household items and maintenance

Although not IoT devices, items such as plugs, sockets, extensions, smoke alarms etc, can be bought with inbuilt cameras or listening devices. Commercially available small cameras and listening devices can also be manually installed into normal household items. Video or audio from these devices can be recorded and/or livestreamed.

Victims of abuse should be wary of items bought by the abuser, especially once they have left the relationship, and inspect such items closely.

If a victim of abuse finds cameras or listening devices in their property, they should report them to the police immediately. While they should save them for evidentiary purposes, they should put them somewhere where they will not give away anything to the abuser.

If the abuser and victim no longer share a home, but the abuser is keen to carry out maintenance or provide items for the home, the victim should be suspicious of their intent. If they need household maintenance doing which they cannot manage themselves, they should ask trusted friends or family for help, or use tradespeople found via personal recommendations or reputable websites.

Bluetooth headphones

Some Apple devices when paired with Bluetooth headphones, such as Airpods and Beats, can use Live Listen. Live Listen enables a phone's microphone to listen to a conversation from a distance or to help hear in a noisy area. This can also be recorded.

This could allow an abuser to eavesdrop into conversations while they are in a different room. They can leave their phone in the room where their victim may be

having a private conversation and listen in. The phone must be within Bluetooth range for this to work.

Victims of domestic abuse should be aware of this possible eavesdropping method if having a sensitive conversation while the abuser is out of the room, but nearby.

All URLs

Two Step Verification (2SV) – Authentication apps

Microsoft: https://www.microsoft.com/en-us/security/mobile-authenticator-app

Google: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en_GB&gl=US