Staying safe online

SafeLives
Ending
domestic
abuse

Technology is an integral part of our lives and while we know it can provide abusive people with tools and opportunities to control, track and abuse, it can also be an important source of support and safety information for victims of abuse.

In the past, safety planning around tech focussed on victims of abuse reducing their use of tech, deleting their social media accounts and getting rid of their smartphone. This is not only unrealistic, it punishes the victim of abuse and cuts them off from their social and support networks, leaving them isolated. Instead, we recommend talking to your clients about using tech safely and taking some simple steps to address potential vulnerabilities. Here are our top tips:

Think about your whole digital footprint

Look at all areas that you use tech in your life and consider if there are any areas in which you would like to improve your understanding, update your security or restrict your visibility.

Be password savvy

Strong passwords are crucial to protecting our accounts. Change user names and passwords, even if you don't think that the accounts have been compromised. You can use a password manager to help with this. You can also consider using two-step verification for added security.

Check security settings

Update security settings on social media accounts so that only the people who you want to connect with can see your posts, photos and information.

Be aware of location settings

Lots of apps and software record information about your geographical location, and this information could be misused by someone with access to your accounts/devices. Check which apps are using location settings and then turn off any that you don't need.

Consider how you might be tracked

There are many ways that tech can allow a person to follow your movements. The most common way is via apps that you have installed yourself, which another person then accesses information from. To minimise the risk of this, consider turning off tracking apps when not in use e.g. 'find my friends/phone/tablet', GPS fitness trackers, sat nav.

Break the connections

Consider any connected or joint accounts that may have been installed on more than one device and could give someone access to your information or devices. This could include accounts for iTunes, app stores, Google Play store, eBay, Amazon, Kindle and others.

Think about tech in the home beyond phones, tablets and computers

Are there 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 or impact you? Change the passwords on these, to ensure that only trusted people can access them.

Secure your home WiFi network

A person may be able to access your devices via the WiFi network, which will be accessible without being inside your home. Change the login details and password so that your network cannot be accessed without your knowledge.

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.