Going online when you're out and about

How to protect yourself, your information and your devices away from the home or office.

GET SAFE ONLINE .org

connected communities

Cheshire East Council

www.getsafeonline.org

As the weather improves and COVID-19 restrictions have largely been lifted, many of us are getting out and about more with our connected devices, whether it's in our personal lives or for work. After all, there's nothing quite like being able to enjoy a coffee when you're working on a spreadsheet or catching up via video call from the park.

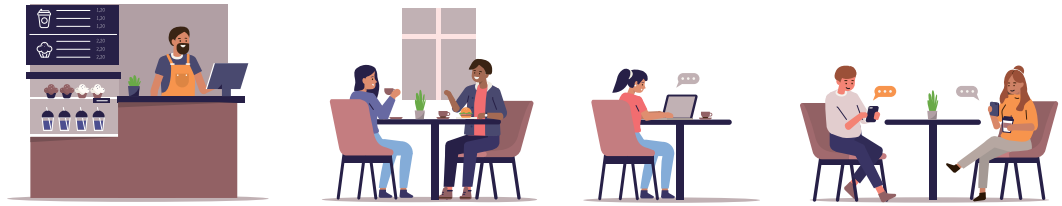
Being online when away from our home or workplace, however, does make it vital to maintain safe and responsible habits and always remain aware of our location and surroundings. If we don't, using our devices away from these relatively secure environments does pose certain risks:

- Your online activity or open apps being incepted via an unsecured or fake Wi-Fi hotspot.
- Your device being accessed via Bluetooth to view your contacts list or access your handset's commands.
- Loss or theft of your device – either when you leave it unattended or while using or carrying it.
- Others dropping unwanted or potentially dangerous or compromised files on your device via features like AirDrop, Nearby Share or third-party mobile file transfer apps.
- 'Shoulder surfing' – when others behind or beside you check out what's on your screen.
- Your screen being viewed and/or recorded by obvious or covert video surveillance.
- Others eavesdropping on your video calls and meetings, either physically or if they've intercepted them online by having the password.

One of the main risks associated with device use in a public place is that Wi-Fi may not be secured, enabling unauthorised interception of anything you are doing online by cybercriminals. The same applies if a bogus Wi-Fi hotspot has been set up to emulate the premises' own network. Entering a key or code supplied by the premises purely provides access and does not indicate security.

Top online safety tips for when you're out and about.

- Never use Wi-Fi hotspots when doing anything **private or sensitive**: they may be insecure, or somebody may have set up a fake hotspot to intercept what you're doing. Instead, use your data or a secure mobile router (dongle), or wait until you can connect to secure Wi-Fi. If you use a VPN (virtual private network), bear in mind that the provider could access your communications.
- Use **Bluetooth and mobile file-sharing apps** with care. Ensure they're switched off when not required. If you do use Bluetooth, make sure your devices are not left 'discoverable'. Don't pair devices in public in case someone is scanning you while you create the connection. Restrict access to known, paired devices. Never accept files transmitted via Bluetooth from unknown or suspicious sources.
- **Never leave devices unattended**, nor in view when not using them, on your seat or table, at the gym, in a vehicle or on public transport.
- Be aware of **who's around you** and may be watching what you are doing online. Consider using a privacy filter which effectively obscures your screen from people sitting either side of you.
- **Avoid getting distracted** by somebody who could steal your device.
- Try not to use your device or have it on show when **walking around**. You could risk becoming a victim of theft and your personal safety could be compromised.
- Don't forget that many apps connect to the internet in the background so you should **check your settings** to be sure of what information is being sent.
- Consider **disabling geolocation on devices and apps** (including social media and fitness apps and your camera). Ensure your home or place of work isn't revealed if the device falls into the wrong hands or its security is compromised.



#outandabout

You can find more information at **www.getsafeonline.org**

Get Safe Online

Get Safe Online is the UK's leading source of information and advice on online safety and security, for the public and small businesses. It is a not-for-profit, public/private sector partnership backed by law enforcement agencies and leading organisations in internet security, banking and retail.

For more information and expert, easy-to-follow, impartial advice on safeguarding yourself, your family, finances, devices and workplace, visit **www.getsafeonline.org**

If you think you've been a victim of online fraud, report it to Action Fraud, the UK's national fraud and cybercrime reporting centre on 0300 123 20 40 or at www.actionfraud.police.uk

In Scotland, report fraud to Police Scotland by calling 101.

GET SAFE ONLINE .org

connected communities

Cheshire East Council

www.getsafeonline.org

OFFICIAL PARTNERS

TESCO · NatWest · Gumtree · Standard Life · first direct · HSBC · Royal Air Force · Royal Bank of Scotland · M&S BANK · LLOYDS BANK · HALIFAX · BANK OF SCOTLAND · creativevirtual · ClearScore · City of London Police · NPCC · National Trading Standards eCrime Team · cifas · EUROPOL EC3 European Cybercrime Centre · ActionFraud · Metropolitan Police · Ofcom · VICTIM SUPPORT · neighbourhood ALERT · Llywodraeth Cymru Welsh Government