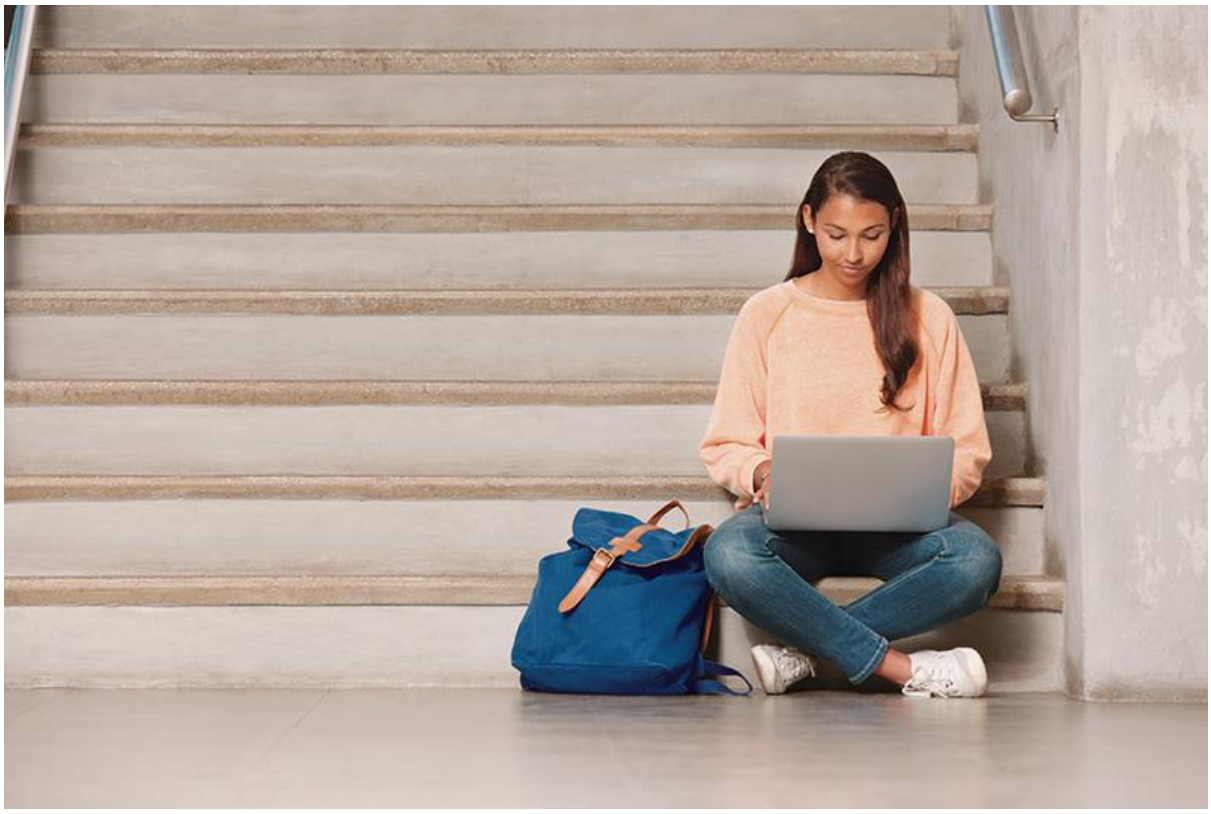
We are here to help you.

Staying Safe Online



Working from home presents many challenges but while everyone is focussing on social distancing and staying safe, it is also a prime time for cyber criminals to target you and/or your company.

With the help of our IT experts, we've put together this handy guide so you can continue to work securely from the comfort of your own home.

Update your WiFi password, especially if you are still using the router's default password. Many hardware vendors publish the default password for their equipment, making it easier than ever for criminals to hack into your home network.

Don't use any work equipment for personal entertainment, such as film or music streaming. Not only can this add unnecessary stress to your work's network, it also opens the network up to hacking.

Be wary of criminals using the COVID-19 pandemic to target you with phishing and phone call scams. These criminals play on your emotional responses and you may see an increase in offers of securing your network or updated guidance about the virus. If you receive any unwarranted emails such as the above, report them as phishing through your work's network or follow your local Government's advice.

Avoid using public WiFi where possible as those without encryption can allow anyone to intercept your browsing in real time, even if you are using the WiFi to remotely connect to your work network. If necessary, use a personal hotspot from your phone to connect to the internet.

Do not use your work email address for personal or non-work-related accounts. You should only look to use your work email for work purposes.

Use encrypted or work-approved platforms for meeting and collaboration with colleagues, such as WebEx or Microsoft Teams. When hosting a virtual meeting, take attendance to ensure there are no intruders on your call.

Mute your smart home assistants, such as Alexa, Amazon Echo and Google Home, while you are working and especially if you are making work-related calls. Whilst you may not have given the word command to activate your device, it can still record your conversations without your knowledge.

Our Timeless Hints

Regardless of whether you are working from home, or a key worker on the go, the following two hints apply to everyone everywhere. We believe they are timeless.

Location Services

Location-based services use real-time data from a device to provide information, entertainment or security. Whilst your location information is vital if you were using a service such as Google Maps, during lockdown this data may compromise your safety as your location data can reveal where you live, your income level based on where you live, your routines and what places you visit.

Whilst many companies use this data legally and safely, any of these technologies can be compromised through signal interception and hijacking, allowing for your data to fall into the wrong hands. Therefore, it is important to understand when it is appropriate for you to enable location sharing.

- **Turn off location services** on all devices where possible.
- **Do not 'check in'** on social media at shops or tag your location while outside your home.
- **Be cautious when giving consent** for apps to collect your location data and review all your current apps to ensure you are happy with the data they collect and what they do with that data.

Passwords

Social media, email, online portals, website subscriptions, online banking, and so much more, all require passwords. Wouldn't life be easier if we could simply use one password for everything? No.

Passwords are there to protect all our information, personal data and everything we own in the digital world. By using one password, you are opening yourself up to someone hacking into all your digital belongings.

Recent research has shown the strongest passwords are a unique and long phrase. For example, 'horsecarrotssaddlestable' is far more secure than using 'P@55w0rd'. Always aim for at least 8 characters and include a combination of letters (upper and lowercase), numbers and symbols (@, £, #, %, &, etc., if allowed).

To further protect yourself, aim to change your password regularly, never use the same password for more than one account and avoid using the 'remember password' feature most websites offer.