BIZCOMMUNITY

Tips for keeping secure whilst working from home

Quentyn Taylor, director of Information Security at Canon for Europe, Middle East & Africa, offers his top tips for keeping secure whilst working from home.

Quentyn Taylor, director of Information Security at Canon for Europe, Middle East & Africa

Phishing for trouble

Cybercriminals are always on the lookout for new opportunities and employees moving outside of the company network offers just that. According to a report by the National Cyber Security Centre in the UK, there has been a significant rise in bogus emails, claiming to offer important updates on safety, which instead infect the user's device with malware.

Make sure to be cautious of emails offering this kind of advice, ensure you check who the sender is and that their email address exactly matches an expected recipient. And if someone is asking you to click on an unknown link – think twice.

Lock up your devices

An occupational hazard of working from home is that your kids now have access to you while you're meant to be at work. They might well be curious about what mom or dad does all day or just want to Google how to make slime.

Either way, they probably don't know that your corporate PC is connected to your company via VPN. So ensure to set boundaries, certain PCs and phones are off-limits to kids.

Print safe

If you're working from home, that probably means you'll be printing at home. But be aware that your home printer is unlikely to have the security features provided by your corporate printers.

While there might be only you and your family in the house, remember that if your printer is connected to the internet, then it's more vulnerable to potential attack. You still need to ensure that your network is private and can only be accessed with a secure password (not 12345).

The other consideration is the secure disposal of documents. Just like you shouldn't throw your bank statements whole into the outdoor bins, you shouldn't be doing that with your company paperwork. Make sure to shred or burn anything confidential once you're ready to get rid of it.

Stay in the loop

Your organisation most likely handles your work device updates. As you're away from the company network, find out what's required to keep your equipment up to date. For example, you might need to leave your laptop on overnight to receive antivirus or Windows updates – your company will advise you.

If you're using your own personal devices, ensure to patch them yourself to get the best security protection available.

Easy does it

Working from home might mean donning your relaxed-wear, whether that's jogging bottoms or even your pyjamas, but that doesn't mean you can relax the company policies. Only use company-provided applications, networks and cloud locations.

As tempting as it can be, avoid free cloud software tools for collaboration and storage which have not been vetted by your organisation. They might be simple to use, but they may not be secure.

If you're working from home, make sure that you have a clear understanding of how to maintain the same level of security, whether you're in the four walls of the office, or on your sofa.