Phriendly Phishing

Remote Working

The traditional office space has been replaced by your house, a cafe, a co-working space, etc. Ensure you understand all the security considerations that come with remote working to keep you and your organisation's data safe.

Virtual Private Network (VPN)

A VPN allows your to work on a secure network by converting all your information into a code, making it difficult for hackers to access.

Public Wi-Fi & Hotspots

Public Wi-Fi and hotspots have limited security, making it easy for hackers to gain access to any sensitive information you send, receive or access while on these networks.

Public Spaces

Scammers can access information from you simply by looking at your screen and typing patterns (otherwise known as 'shoulder surfing'). Be aware of your surroundings when working remote, and never leave your device unattended in public spaces.

Two-Factor Authentication

Whenever possible, use two-factor authentication when you connect online. This requires two ways of proving your identity, adding another layer of security which can protect your accounts and data.

Passphrases

The password "Password" takes just 0.29 milliseconds to crack. Hackers use a range of tools to crack passwords in record times. Consider updating your passwords to passphrases; they are easy to remember and more difficult to hack.

Software Updates & Data Backups

If your computer breaks, gets hacked or you're locked out, your data may be gone forever. Ensure you backup your files regularly to prevent any data loss or fix and flaws corrected by your software vendors.