9 CYBER SAFETY TIPS FOR YOUR EMPLOYEES

#1 Do Not Ignore Updates

Your operating system and your anti-virus software should be updated regularly/every time they are available.

Do not forget your phone/mobile devices as well if you use them for work.

Most updates are released to tighten security or prevent known malicious software from accessing your systems and data, so this step is crucial.

#2 Choose Strong Passwords. Change Them Regularly

Even the most advance anti-virus software cannot do much for you if your password is “pasword123”, or if it is on a “post-it” left on your screen, or if is the name of your dog, which you post about all the time on social media.

Passwords that are hard to guess, with more than 12 characters, mix of symbols, numbers and upper and lower case letters are best.

#3 Do not leave your devices unattended

Set up screen lock at sensible times so no one can access your device and data even if you are engaged elsewhere unexpectedly.

#4 Avoid Using Free or Public Wi-Fi as much as possible

If you absolutely have to do it, then make sure you delete the network after that, so your devices do not login automatically again if you find yourself in range.

#5 Do Not Ignore Warnings About Pages and Websites

Ask us about ad blockers or plug-ins we can install that will keep these from even loading.

There are also solutions that can check the links and display alerts on your Google searches, so you can browse safer.

#6 Keep Sensitive Data to the Minimum on Your Device

Make sure that you keep only data that you need at the moment or use on a regular basis synced on your work device.

All data not in use should be backed up and deleted from workstations to minimise the impact of any breaches and protect client data and privacy.

#7 Be Suspicions of Emails From People You Do Not Know

Double check the name and the domain of the sender email match the person in the signature.

Emails from services such as Gmail or Hotmail, but claiming they represent a business or a government body, or ones from domains with spelling errors, should not be responded to.

Do not click on links or open attachments when you do not know the sender or you have not requested the document yourself that they are providing.

#8 Always Verify Independently

Always type your bank’s URL in the browser yourself (or any other online service you use, such as your accounting software, or government agency such as IRD), and never follow email or website links to access these services.

Always look up the contacts details online and never use the contact details in the signature if you have to verify the sender.

#9 When In Doubt, Do Contact Us Right Away

We are here to help and sort these issues for you. Please forward the suspicious email as soon as you see it or ring our help desk right away if you are worried your system might be at risk.

As your IT team, we will look into it and make sure that your network is safe and all necessary precautions are in place. We really need to be aware of these issues and investigate all instances of suspicious behaviour, so do let us know if you have been targeted.