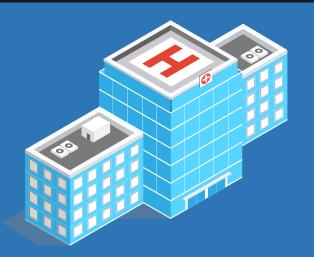


Cyber Security Notice

27 March 2020



You may have heard that ransomware cybercrime gangs promise to give healthcare a free pass. This is **not** the case. Cyber security companies around the world are in fact seeing an increase in cybercrime capitalising on the Covid-19 pandemic.

Ransomware continues to be one of the most severe threats facing organisations of all kinds, especially as attack methods continue to evolve.

Please read the information below which highlights good practice while working from home and how to mitigate the risk of your computer from being hacked or infected.

If you suspect your login credentials or your computer might have been compromised, please call the ICT Service Desk on 04 918 6146

Five tips to protect your computer from internet threats at home

Do not give sensitive information to others unless you are sure that they are indeed who they claim to be

Don't give out your user name and password

If a website asks for your user name and password, check:

- Is the website name is spelt correctly?
- Is the website is secure? look for a closed padlock
- Don't use a website that warns you of certificate errors

Ensure your computer has all the latest updates installed

If using Windows, make sure Windows Firewall is active

Security and privacy reminders for staff working from home



Your obligations to protect personal information remain irrespective of your workplace location

Don't send personal patient information through social media or WhatsApp groups





Work from a secure private Wi-Fi instead of a public access Wi-Fi

When video conferencing, be mindful of information that's being captured and presented. Also ensure there is no sensitive, identifying or inappropriate information captured in the video. background unintentionally





If you are using your home computer to access work files, ensure that your computer has the latest anti-virus software and system updates

Don't use outside email services, such as Gmail, to send or access work content





If taking patient or staff paper notes home, ensure that these are securely stored when at home and during transit

Be mindful of information that is in hard copy or printed at home – if this needs to be destroyed please ensure that the documents are stored securely and shredded before being thrown away





Working at home, be mindful where you have conversations and be cognisant of those around you to ensure the confidentiality of the information

Access work information through the secure Citrix desktops provided by the DHB's





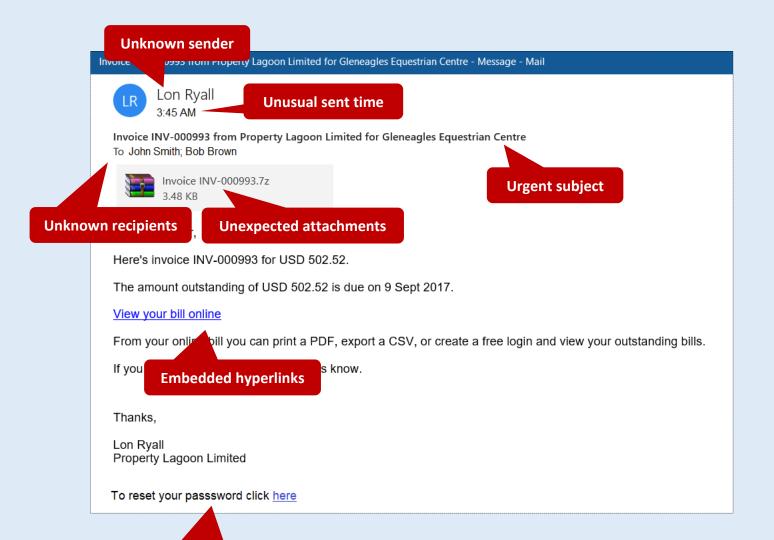
Beware of coronavirus-themed phishing emails - do not **click**, do not **access** and don't forget to **report**

If in doubt contact the Privacy Officer at privacy@ccdhb.org.nz or see the Office of the Privacy Commissioners "On the Road" Guideline at https://www.privacy.org.nz/news-and-publications/guidance-resources/health-on-the-road/





Red flags to look out for in email



Password changes, spelling and grammatical errors