Top Tips for Staying Safe Online

Cybercrime is on the increase around the globe and COVID lockdowns are helping criminals prey on vulnerable individuals who may be struggling financially, feeling isolated and looking for comfort or company or stressed out juggling childcare and work responsibilities.

Where to start? Cybersecurity researcher Chris Hails has compiled the following 'baker's dozen' to provide you with a step by step plan to put in place key digital defences:

1. Identify your digital 'crown jewels'

- You can't secure everything so focus your efforts on what matters most.
- Obvious candidates include your primary computer, your smartphone and account logins for important systems like internet banking and any other platforms that store your credit card or payment information.
- Take 10minutes to think carefully about the systems, services and information you rely on and make a list of what to secure first.

2. Back up what's important to you

Step 1 will help you identify things you've invested time in creating or have an emotional attachment to. Digital photos, key business documents, and your family tree research - everyone has something that could be irreplaceable if lost to a digital disaster like a malware infection, disk failure or compromised account.

A burglary might also see your laptop stolen and that only draft of your first novel lost forever. A $20 USB stick, external hard drive and cloud backup can all help you plan for the worst case scenario – think...

- 3 copies of your key data in
- 2 different formats with at least
- 1 copy off-site.

3. Identify vulnerable family and friends

As you start to secure your own 'crown jewels' and take steps to avoid becoming a victim of cybercrime, think about friends, neighbours and family members who might also benefit from your growing expertise.

Older Kiwis can often be targeted by overseas phone scammers who autodial landline phone numbers and hope to exploit a friendly caller. And anyone can fall victim to an email or txt scam - if they haven't been warned to watch out. Think of the recent FluBot and COVID testing notifications arriving on devices around the country.

Sign up for notifications from CERT NZ www.cert.govt.nz and NZ Police www.police.govt.nz and talk with those you consider might be at higher risk of falling victim.

Top Tips for Staying Safe Online

4. Check your digital footprint

Cybercriminals may seek out easy targets by combing through social media postings, building up a profile of business owners and learning what makes them tick. International research has shown it's easier to trick someone by pretending to be a friend or former colleague, by mentioning a shared interest or hobby or claiming a connection.

Spend 5 minutes Googling your own name and you may be surprised at how much information there is out there online about you. Take a cautious approach and avoid oversharing personal information, photos and details about travel or holidays that might reveal your location, lifestyle or other data that could give away account passwords or security question information like your date of birth, school or the name of your dog! (We hope your password is longer and stronger than 'F1d0').

5. Review your privacy settings

Once you know how much information you've published in the past, look to remove what you can and use platform privacy settings to lockdown who can see your status, pictures and updates. Your Android or iOS phone also has settings that can limit sharing of location data and block apps from harvesting information about your online activities. A quick Google can help you find device guides to follow.

6. Use strong, unique passwords

Long and strong passwords are much harder for attackers to crack. We recommend creating a passphrase, that's a string of four or more words as it's easier to remember and is stronger than a random mix of letters, numbers and symbols.

7. Protect your key accounts with 2FA

It's a simple extra step after you log in, like using your thumb print or entering a code from an app.

8. Protect all your devices

Tips 6, 7 and 8 match the advice provided as part of NZ's Cyber Smart Week 2021

Using a password manager like 1Password, Dashlane, Bitwarden or Lastpass is another top tip for helping you securely manage those dozens of logins www.cert.govt.nz Upgrading to two-factor authentication ('2FA' or sometimes MFA) adds another layer of protection to your accounts and can involve receiving a login code by text or linking an Authenticator app to your account. More info at www.cert.govt.nz

To protect your devices make sure you apply software updates as soon as you can www.cert.govt.nz and keep your systems 'patched'. Going online with older technology can leave you more vulnerable to viruses and malware as security holes become known about in older operating systems and can be exploited through just a click or by visiting a malicious website.

9. Slow down and frown

Top Tips for Staying Safe Online

10. Think before you click

11. Research any online offer

We're into the behavioural aspects of cybercrime prevention now where engaging your brain is key! Most of us will know that being stressed, under time pressure or worried about things leave us open to making mistakes. This applies to many aspects of everyday life and not just when reading your emails or studying a suspicious txt message.

Researchers have shown that frowning when reading makes the brain more alert to threats and increases a sense of vigilance. Next time you're unsure about a message received try reading it out loud with a frown on your face and see if any red flags are raised.

Taking a moment to stop and think before giving out personal or payment information could also keep you safe. The UK's 'Take Five to Stop Fraud' campaign encourages everyone to challenge odd or urgent requests and highlights that only criminals will try to rush or panic you into clicking links or submitting account information online.

If frowning or pausing to consider that parcel delivery txt message or amazingly cheap online shopping bargain makes you suspicious, research the company, the website URL or parts of the message content further by searching online or talking with friends and family. Look before you leap and you could avoid a nasty surprise, especially if others have already experienced the downside.

12. Create an incident response plan

'Be Prepared' has been the Scouts motto for over a 100 years and is just as valuable in the 21st Century. Your 'crown jewels' list has shown you what needs the most protection, now create another list for ways to get help if something does go wrong. Add NZ Police's '105' phone number for non-emergency assistance, the 105.police.govt.nz website and the phone number for your bank's fraud team - it may be on the back of your EFTPOS card. Stopping a payment or reporting a possible fraud is the best course of action if you think you may have been scammed and the quicker you report it the better. IDCARE are another handy source of advice and have prevention tips too www.idcare.org on protecting your credit report, identity documents like your driving licence and your mobile phone SIM too.

13. Keep your clothes on

Our last tip is voluntary but comes from assisting victims of 'sextortion' in the past. Stripping off, sharing your birthday suit pics or appearing naked on camera is down to personal choice and risk appetite. Just be aware that there are criminals out there who specialize in tricking people into oversharing on video calls and then blackmailing them with recordings. It's not a pleasant place to find yourself being held to ransom so plan ahead and keep that webcam covered when it's not required.