





HOW SAFE ARE YOU ONLINE?

In today's digital world where we rely on the Internet for our work, we all need to take steps to keep our information and access to our IT systems safe. So what should we do to protect ourselves? This handy guide lists 10 recommended actions you should take to stay safe.

Produced by

.DigitalJourney

 03 366 9596  www.digitaljourney.org

01 PASSWORDS

Do you leave your front door unlocked? Most of us don't. We lock our door with a key to keep the bad guys out.

The same logic applies to your devices. It's important that you safeguard access to your computer and smartphone, and that you create passwords that will not be easily guessed. Remember, you shouldn't write down passwords in a notebook! That's like leaving your keys under your front door mat!

TIP
Use a different password for every online account. Make it long and hard to guess! Like 'Todaywasagreatday'. Or look into a password manager which allows you to remember one set of login details to access all your passwords. You can use a password manager on your phone, tablet or computer. www.lastpass.com is worth checking out.

02 VIRUSES

Viruses can infect your computer in more than one way.

A link you click in an email, a website that's infected with a virus or even a Facebook message. It's essential you have a virus protector installed on all your devices. Choose a reputable brand and ensure it's regularly updated. If you use Windows, Microsoft Defender antivirus can be used. There are plenty out there to research and buy.

TIP
Don't forget about your smartphone. Look at virus protection that covers all your devices. Check your Windows PC is operating securely. Type 'security' in the search bar to see how it's set up.

03 UPDATING SOFTWARE

Those annoying updates to our software are actually very important.

Updating software is important as cybercriminals will exploit weaknesses in software to gain control. Always ensure your software is the latest version available. Some older versions of Windows or other operating systems struggle with updates, which may increase risk. It may be time to consider an upgrade to a new machine with the latest operating system which will be far more secure!

TIP
Keeping your browser up to date is key. To check and see if your browser is operating at the latest version go to www.whatismybrowser.com

04 TWO-FACTOR AUTHENTICATION

Set up a double check on login! Sounds confusing, but this is a great tool.

This is a great way to prevent access to your personal information, social media and emails. It's like having two locks on your front door! How it works is that you need two pieces of information to log in to your accounts, your password and a secret code that is typically sent to your phone. This means that if a hacker manages to find out your password they still can't login, as they need the secret code sent to your phone! Crafty eh? And a great way to keep your information secure. Services like Gmail, Office 365, Xero accounts and Facebook all offer this service.

TIP
Keen to use 2 Factor Authentication? Check out this website to see which providers support this service: www.twofactorauth.org

05 SOCIAL MEDIA PRIVACY

Social media can give cyber criminals information that they can use against you.

Facebook is by far the most popular social media service in NZ, your privacy settings are therefore very important. What information you share on social media needs to be carefully considered. For example, on some websites, you can choose your password recovery by answering questions like 'What was the last school you attended?'. For a hacker, if this information was shared on Facebook, it could be an easy hack.

TIP

Make sure to check the privacy settings on Facebook by going to Settings/Privacy. Also "View As" to see how your Facebook page looks to others.

06 PHISHING FOR YOUR DETAILS!

Another sneaky way that hackers try to steal information is through emails that pretend to be legitimate.

Organisations won't ever ask you to verify personal information in an email form. A common scam is an email from your bank asking you to verify your account details. It may look authentic but this is the way hackers will tempt you into providing information like your usernames/password or to try and get you to click a link which will infect your computer with a virus. If you receive an email asking for personal details, get in touch with the organisation who sent it and check that it's genuine.

TIP

Set up an email address which you can use solely for signing up to services. This way you limit who knows your real address.

07 FREE WI-FI HOTSPOTS

Be careful of free Wi-fi available in public places offering access to the Internet.

This can be used by hackers to steal passwords or access private information. It's vital to check what hot spot you are accessing before using the service. It's very easy for a hacker to set up a Wi-Fi hot spot at airports, cafes or hotels and collect account details or credit card information! Some anti-virus products or your IT team may have set up a 'Virtual Private Tunnel' which will keep your internet use private.

TIP

Avoid online shopping, banking and emailing while on a public Wi-Fi hotspot.

08 SAFE SHOPPING!

It's so easy now to buy things online!

There are fake shopping sites or websites out there that contain malware to infect your computer. To stay safe we recommend the following:

TIP

- Use only shopping sites you trust and are well-known. Avoid shopping sites you find through an online search.
- Look for a secure site, especially when you're using your credit card. It's your responsibility to check that the site is secure. You can tell by the web address. It will begin with HTTPS:// and not just HTTP://. An icon of a locked padlock will appear next to the URL in the address bar and the status bar at the bottom of the web browser.
- Use a credit card with a low credit limit. Or use a Prezy Card which has a set limit on it.

09 BACK UP!

The most important tip - one that everyone should follow.

You just never know if your computer and your data will be impacted by a virus. A regular backup of your data onto an external hard-drive that's disconnected from your computer or with an online backup service could be a lifesaver.

TIP

A virus infected computer could be wiped clean and your backup used to restore your data! Backup regularly!

10 "WHO YOU GONNA CALL?"

If you've been impacted by cyber crime then you can get help.

You can contact CERT NZ - www.cert.govt.nz, or if you are being cyber bullied go to www.netsafe.org.nz. Finally, for more information and advice check out our free online knowledge base:

www.digitalresources.nz (search cyber)

TIP

Go to www.havebeenpwned.com to see if your email has been hacked. If it has, then change your login/password and look at using 2 factor authentication.



.DigitalJourney
www.digitaljourney.org