connect SMART
Protect yourself online

newzealand.govt.nz

Connect Smart is about raising awareness of cyber security and promoting ways to protect yourself online. All New Zealanders will benefit if we can fully unlock the potential of the internet by using it in a safe and secure way – in other words, learn to Connect Smart.

## Connect Smart – protect yourself online

1. Don't wait until it's too late – be proactive; improve your digital security now before you become a victim.
2. Improving your digital security is easy – it's not complicated or expensive to take basic steps to protect yourself and your personal information.
3. Protect yourself across all your devices – it's as important to be secure on your smartphone and tablet as it is on your PC or laptop.
4. Protecting yourself also protects friends, family and work – having your personal information compromised is more than an inconvenience and can have major consequences for you and everybody you know.

## How do I protect myself online?

### Passwords

- Make sure all your internet devices, e.g. desktop computers, laptops, tablets, and mobile phones, are all secured with different passwords.
- Use strong or complex passwords (by including a range of upper and lower case letters, numbers and punctuation), particularly for your email and online banking.
- Change these passwords regularly.

### Wifi

- Make sure your wireless connections are secure – protect them with a strong password and encryption.
- If you are operating on an unsecured wifi, be cautious about what you do. Don't use unsecured wifi for banking or other transactions.

### Emails & Social Media

- Be suspicious of emails from people you don't know or that look unusual. It may be spam email with malicious software attached.
- Be suspicious of links to unknown websites. If you are not sure, don't click on them. Only visit trusted or reputable sites.
- Limit the amount and type of identity information you share about yourself, friends or family through email or online.
- Check your privacy settings on social media sites.

### Computer Security

- Install adequate firewalls.
- Keep your anti-virus software up-to-date.
- Ensure your operating software is up to date.
- Ensure that you have information safely backed-up should anything happen. If disposing of a computer, make sure you have removed all personal data and take steps to clean the hard drive.

### Mobile Devices

- Secure it with a password.
- As with your other internet devices, use anti-virus software and have up to date software.
- Only download reputable apps.

### Online Shopping

- When shopping online, use a secure payment method or your credit card, and don't make payments on unsecured wifi.
- Be aware of scams, online frauds and false suppliers.
- Make sure that requests from companies or individuals for identity or financial information is authentic.