CYBER CURE+
cyber security starts with us

October 31 2023

Cyber Smart Week is here!

Many New Zealanders know the risks of cybercrime, but they don’t always take the steps to keep themselves safe.

To show how anyone can be vulnerable online, CERT NZ is presenting a photo exhibition called EXPOSED. It features real people who have been victims of cyber attacks while using the internet. These stories show the impact of cybercrime, to encourage others to protect themselves online.

Install Software Updates

Keeping your devices and software up-to-date is one of the most effective things you can do to keep your systems safe.

Devices and software that are not up-to-date are at risk of attacks. Software updates (also known as patches) don't just add new features – they often fix security vulnerabilities too.

Implement MFA

Implementing MFA means that anyone who logs in to your system will need to provide something on top of their username and password to verify that they are who they say they are. You can implement MFA on internal systems and your customer-facing systems.

Using MFA can reduce the risk of credential reuse, phishing attacks, and many other online security threats.

Back Up Your Data

Backups are a copy of your data – all the digital information you need to keep your business running. You can store backups in the cloud or offline, and should run them regularly.

If your business data is compromised in any way — if it’s lost, leaked or stolen, for example — the backup lets you restore it quickly so your business can keep running.

Create a Plan

If your business has a cyber security incident, you’ll need to know what steps to take to keep your business running.

Having a clear plan in place will help you through what could be a stressful time. It’ll help your team respond to an incident quickly, and improve your business's resilience.