Mobile security is a must!

Are you being Data Smart with your Smart Phone?

Recently, the new shiny iPhone XS and XR entered the market.

For all the Apple lovers out there, this might mean being the first to wrap your hands around the irresistibly smooth all-glass design, or finally upgrading your old glitchy iPhone to the new model.

If this is you, I'm guessing you're focused on the opportunity to start afresh, buy a new case, clear all those apps cluttering your current device, and start playing with its new features. Right?

But have you considered the security aspects?

According to online security software vendor, Norton, the scary reality is that 978 million people in 20 countries were affected by cybercrime in 2017. In New Zealand and Australia, one in four small businesses experienced a cyber-attack or hacking attempt.

"It's an unfortunate fact that the impact of cybercrime is a reality for all businesses," Xero Head of Security, Paul Macpherson, said at the recent Xerocon conference in Brisbane. "We continually remind all of our customers – small businesses, accountants and bookkeepers – to take precautions to keep their data safe from hackers." Sure, you'll be eager to try the cool Face ID feature and of course you wouldn't dream of breaking your shiny new phone. But are you mindful of how you'll keep its contents safe too?

Obtaining a new phone is the perfect opportunity to get everything set up correctly right from the start. And if you don't plan to upgrade your mobile phone, there's no time like the present to make changes.

ARE YOU TOO RELAXED WITH YOUR DATA SECURITY?

While many of us are looking for convenience of easy-to-find or easy-to-remember passwords, in reality you're making yourself vulnerable to digital identity theft.

Xero Head of Industry, Matthew Prouse, says "the biggest mistake people make is keep highly confidential information in their phone, such as in 'Notes' or disguised as a contact. You're walking around with a pocket of very sensitive data."

Prouse recommends that you **do not** –

- Add passwords and pin codes to the 'Notes' app
- Try to disguise passwords, bank account numbers or your tax file number as phone contacts
- Choose obvious passwords (such as your date of birth or cat's name) that even your kids can work out
- Replicate the same codes everywhere (such as your bank account pin)
- Allow your computer or phone to automatically save passwords
- Hand over old mobile phones to your kids without clearing all sensitive data first

Think about the worst case scenario: your phone gets stolen. For many of us, this doesn't just mean losing a device. It also means losing passwords. And your digital identity.

Every day, there are reports of email accounts being hacked, phishing emails being sent with the aim of collecting credit card details and bank account numbers, and credentials stolen from one website and then used against other sites to see if username and passwords have been replicated.

Macpherson says over 80% of breaches occur via stolen or weak passwords, with email as the primary method of attack. So it's highly important to keep sensitive employee and customer data safe via modern security practices, especially while running a sustainable and trusted modern business.

HOW CAN I IMPROVE MY MOBILE PHONE SECURITY?

Now is the time to brush up on your security awareness.

Prouse recommends utilising apps such as **LastPass** and **Google Authenticator** for encryption and a second layer of security for important business and personal websites. However, you can't just download them and consider yourself completely covered.

"As a business owner, your smartphone itself needs to be safe and secure too," says Prouse. "Make sure there is a fingerprint scanner, facial recognition, and good password security."

And when it comes to passwords, Prouse suggests thinking outside the box.

"You might like to check out Stay Smart Online for some good tips and policies around passwords. Don't just use your date of birth, postcode, or banking pin numbers. Pick random numbers; the authorisation apps will remember them for you."

It's also key to remember that if you have an existing authenticator app setup on your old phone, you need to set it up on your new device before disposing of your old one.

So if you're getting your hands on the new iPhone X, take some time to set up the security as a priority. Because, admit it, downloading Instagram was otherwise first on your list!