Te Whatu Ora
Health New Zealand

Information

Cyber security incidents can cause significant harm to your organisation and have long term impacts.

This article talks about some common cyber threats and what you can do to protect your organisation, now and in the future.

COMMON THREATS

Malicious Software

Also called 'Malware', it's software that cyber criminals use to spy on your devices or even take control of them.

Ransomware

It's a type of malware that locks up or encrypts your files so you can't access them. It can also completely stop your devices or system from working.

Cyber criminals then ask you to pay money to get your files unlocked. If you are the victim of a ransomware attack, don't pay.

Contact CERT NZ for help on www.cert.govt.nz/report or 0800 CERT NZ.

Identify theft

It's where someone pretends to be you online. They use your details to steal personal or organisational information and use it to their benefit.

TOPICS

Common threats

What are the most common cyber security threats facing small organisations now?

What you can do about it

Some things you can do to protect your organisation against the common threats.

This includes taking the time to review unexpected emails and text messages, using strong passwords, and keeping your devices up to date.

COMMON THREATS

Phishing is where cyber criminals try and trick you into giving them information or access to your organisations system(s).

Like pretending that your bank account has been locked and you need to re-enter your credentials.

Phishing attacks can come as fake emails, text messages (smishing) or phone calls (vishing) and sometimes as a combination of all three.

These attacks are on the increase, and they are becoming harder to spot.

WHAT TO DO ABOUT IT

Turn on automatic updates for all your devices and software. Updates include protections against malware and 'plug' any security gaps that have been identified. Windows and apple support pages have instructions on how to turn them on.

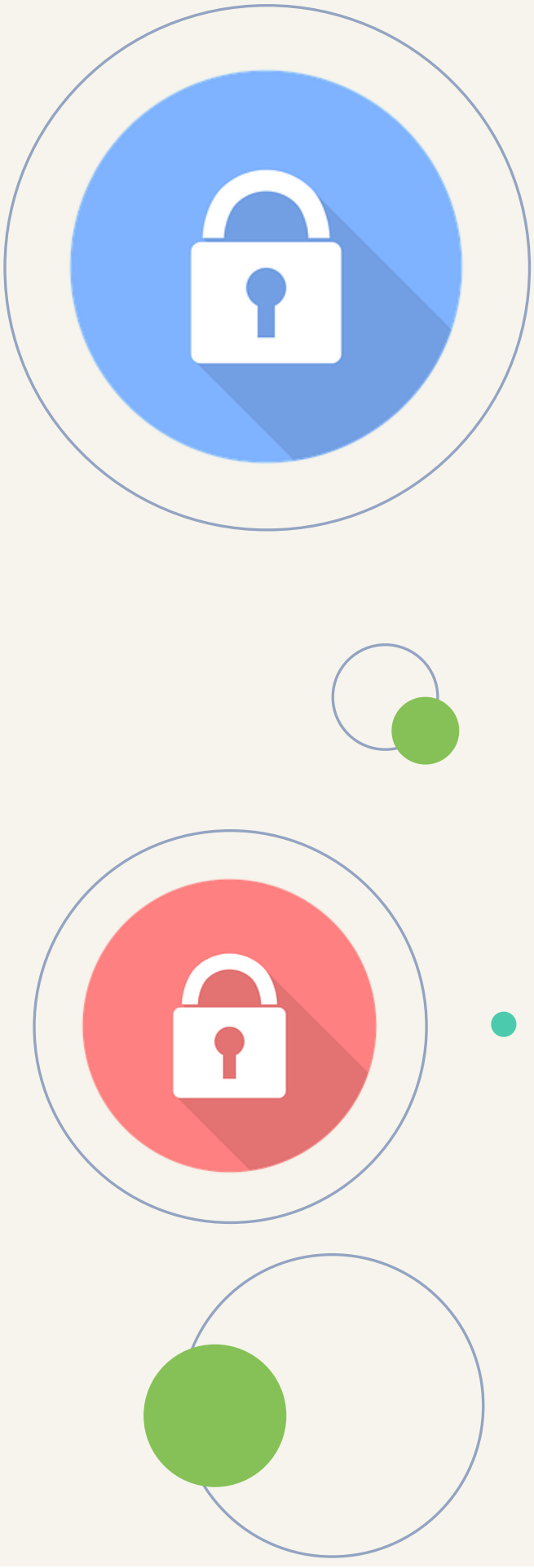
Take time to consider unsolicited emails, text messages and phone calls. Look for:

- ***Sense of urgency*** – is it time pressured in any way? Do you have to respond now?
- ***To good to be true*** – is this a super good deal, great offer, or gift?
- ***Position of authority*** – is it coming from someone senior in your organisation or a Government agency?
- ***Unexpected*** – is this unsolicited or out of the ordinary?

If in doubt, don't click on any links. You can contact the person/agency the email is from and verify it or contact CERT NZ for help.

https://www.cert.govt.nz/individuals/common-threats/

Be wary of any unsolicited emails, phone calls or text messages!



WHAT TO DO ABOUT IT

Back up your data regularly, taking a digital copy of your data and storing it somewhere else is like an insurance policy for your data and it can help your organisation recovery quickly from a ransomware attack.

Find a back-up system that works for your organisation. And test your back up process. Always keep at least one back up copy offsite and ensure it is not connected to your network.

Create long strong passwords consisting of three to four random words instead of short ones as these are harder for cyber criminals to guess. Each password should be unique and not contain family details.

Use a password manager A password manager is an application that provides suggestions and stores all your passwords – like an online safe. There are lots of different password managers available. Work out what features are important to you and find one that suits.

Use multi factor authentication (MFA) which is a combination of something you know (your password) and something you have, like your cell phone or something you are, like your face or your fingerprint. The multiple levels of authentication make it harder for cyber criminals to attack your organisation.

There are several types of MFA available like: physical tokens/cards, authenticator apps, email, and text confirmations, etc. Find a method that works for your organisation and implement it.

Access control – be mindful of who has access to what information and systems in your organisation. Work on the principle of the least amount of access needed to perform any given task or activity. Make sure to remove access when people leave your organisation.

Train your staff and keep up to date – train your staff on how to create strong passwords, use MFA and spot phishing attacks. Keep up to date on new and emerging cyber security threats. Ensure training also includes the dangers of sharing passwords and reusing them across multiple accounts.

Subscribe to CERT NZ to receive updates on the latest threats and information on how to stay secure.

https://www.cert.govt.nz/business/