PHISHING TOP TIPS

PROTECTING YOURSELF FROM PHISHING THREATS

What is phishing?

Phishing is a type of scam, typically via email. The sender pretends to be from a trustworthy organisation in an attempt to get you to share sensitive information.

The vast majority of successful data breaches are a result of phishing.

Phishing scams often ask for:

- Usernames or passwords for your online accounts
- Your credit card information
- Your internet banking details
- Personal information and documents

Attackers send phishing scams to many recipients, made up of contact details found on web pages and social media sites, or from other lists that are shared and sold online. In some cases they use guesswork, and send phishing emails to addresses that might be in use in the hope that they'll reach someone's inbox.

Most phishing scams look like they come from:

- A bank
- A social media site
- A government agency
- An online game, or
- An online service with access to your financial details, like iTunes.

Phishing scams may ask you to either click a link or open an attachment. This will prompt you to enter personal information somewhere online, or allow the sender to infect your device with malware. Either way, this gives them access to your personal information without you knowing.

It's important to know that reputable organisations will never ask you to provide them with personal information by email or text.

If you've received a phishing scam...

If you haven't done anything with the scam, delete it.

If you gave out some personal or financial details:

- ✓ **Contact the service provider** for your online accounts — like your bank or your email provider. Let them know what's happened and ask what they can do to help.
- ✓ **Change the passwords** for any online accounts you think might be at risk.
- ✓ **Get a credit check done** to see if any accounts have been opened in your name. There are 3 main credit check companies in NZ, and you'll have to contact all of them. You can ask to have your credit record corrected if there's any suspicious activity on it.

FARM SOURCE

Fonterra

Dairy for life

Preventing phishing

Although you can't prevent a phishing attack, there are things you can do to make sure you recognise one.

- Know what to look for in a phishing scam. You might notice that:

⚠ You don't recognise the sender
⚠ The sender name doesn't seem quite right
⚠ You don't recognise the organisation's name
⚠ The logo doesn't look like it should
⚠ The scam refers to you in a generic or odd way
⚠ The scam contains bad grammar or spelling
⚠ In emails: If you hover over a link with your mouse, the address that you see doesn't match the place the email says it will take you

- Don't click on web links sent by someone you don't know, or that seem out of character for someone you do know. If you're not sure about something, contact the person you think might have sent it to check first.
- Use bookmarks or favourites to access websites rather than links in emails.
- Check to see how the companies you deal with — like your bank — will contact you, so you're more likely to recognise what's a legitimate request and what isn't.
- If you have your own business, make sure you keep your support contracts up to date (with your antivirus provider or your firewall provider, for example).

REMEMBER — if you don't click on any links or attachments in a phishing scam, your system is safe.

Where to go for more information related to cybersecurity?

At Farm Source, we are working and communicating with our community to ensure they also act as our first line of defence against cybersecurity incidents.

If you do see something suspicious or need more support around staying cyber safe, we recommend the following resources:

- **https://www.cert.govt.nz – Cert NZ** has great resources and tips on how you and your family can stay cyber safe, as well as updates on the latest scams
- Follow **NetSafe NZ** on **social media** for the latest advice, great cyber resources and tips for business and families
- Get in touch with our **Service Centre** on **0800 65 65 68** in the first instance if you have any specific cyber security concerns related to Farm Source