Cyber safety

Protecting your practice against phishing

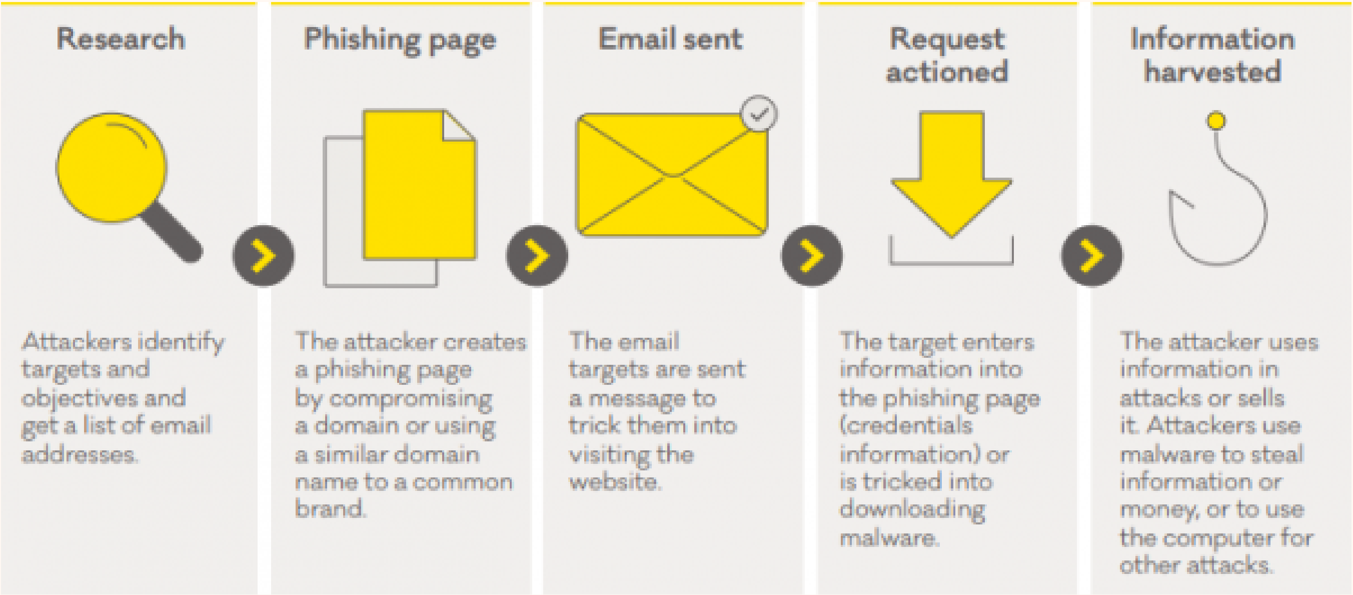
Mahitahi Hauora

The recent cyber attack against Pinnacle Health is a reminder of the need to remain vigilant about cyber security.

One of the most common cyber threats is phishing. Phishing attacks can enable cyber criminals to obtain user credentials that allow them access to an organisation's systems.

What is phishing?

Phishing is a type of email scam. The sender pretends to be a trustworthy organisation, and the email will ask the recipient to click on a link or open an attachment. This may prompt the recipient to enter personal information online, or it may allow the sender to infect the recipient's systems with malware. In this way, the sender gains access to private information and systems without the recipient knowing.



Research

Attackers identify targets and objectives and get a list of email addresses.

Phishing page

The attacker creates a phishing page by compromising a domain or using a similar domain name to a common brand.

Email sent

The email targets are sent a message to trick them into visiting the website.

Request actioned

The target enters information into the phishing page (credentials information) or is tricked into downloading malware.

Information harvested

The attacker uses information in attacks or sells it. Attackers use malware to steal information or money, or to use the computer for other attacks.

Source: CERT NZ - Phishing scams and your business | CERT NZ

How to deal with phishing attacks

Staff education and training

It's important that everyone using your systems is aware of phishing attacks and understands the risk they pose to the organisation.

Make sure your team know how to recognise a phishing email. Signs an email may be a phishing attack include:

- You don't recognise the sender, the name of the company, or the sender's name or company logo doesn't look or sound quite right.
- The email refers to you in a generic way.
- The email contains bad spelling or grammar.
- If you hover over a link in the email with your mouse, you'll see a URL – it this URL doesn't match the place the email says the link will take you, it could be a phishing attack.

Your team should know what to do if they receive a suspected phishing email.

- Never click on any links or attachments in a phishing email.
- Report the email immediately to your IT team or provider – make sure everyone knows who to contact.

Security policies and systems

- Make sure you have adequate policies for access requirements to your system, such as multi-factor authentication. Multi-factor authentication means additional verification is required when attempting to access critical systems or carry out sensitive processes.
- Subscribe to a mail gateway service that scans incoming email before it arrives in staff inboxes.
- Ensure you have antivirus protection installed on all systems and keep it up-to-date.
- Back up your servers regularly and have a testing schedule.

Monitoring

- Have systems in place to be able to review user/device activity. Carry out reviews regularly so you can identify any abnormal trends.

Useful links and contacts

CERT NZ is a Government organisation that supports businesses, organisations and individuals affected by cyber security incidents. Their website, www.cert.govt.nz, provides a lot of useful information and advice:

- Phishing scams and your business | CERT NZ
- Phishing | CERT NZ
- Guides – Protect your business from cyber security risks | CERT NZ
- Cyber security quiz | CERT NZ

CERT NZ also has an email address you can forward suspected phishing attacks to: phishpond@ops.cert.govt.nz