emergence

social engineering

Exploiting humans

Social engineering is the practice of tricking or duping people into doing something they wouldn't normally do, when using technology. It also manipulates people into performing actions or divulging confidential information.

Social Engineering attacks continue to increase each year. It can be very sophisticated, and many businesses only realise they've been duped once it's too late. Here are four easy ways to protect yourself from a social engineering attack.

Think before you click

A good rule of thumb is that if it doesn't seem right, don't open it! This applies not only to attachments but if there are certain links in an email asking you to click to go somewhere. Hover over the link to look at the URL and use a search engine to determine its validity.

Secured websites

Only make financial transactions that are known to you and are on secured websites (e.g. URL beginning with "https" and/or look for the padlock symbol)

Confirmation

Changes to financial / banking details NEED to be re-confirmed. Pick up the phone and call the contact (from your existing details). When calling, whoever you're speaking with to confirm any details that have been changed.

Slow down

In our fast-paced world, everything appears URGENT. Ensure you still take the necessary time to review what exactly you are being asked to do or complete. This will help to reduce the likelihood of you being time pressured into making errors.

ENHANCE YOUR SECURITY

Without adequate safeguards, experiencing a Cyber Event is less a matter of *'if'*, and rather, more a matter of *'when'*. To ensure that you are as protected as possible against a Cyber Event, use the following checklist to see how many safeguards you already have in place in your business.

- ☑ Daily off-line backups of data and business critical information with regular testing of backup.
- ☑ Using Password Manager programs.
- ☑ Enabling multi-factor authentication.
- ☑ Tested Business Continuity Plan (BCP) and/or Disaster Recovery Plan (DRP).
- ☑ Antivirus software (updated daily or upon release).
- ☑ Firewalls.
- ☑ Intrusion Prevention / Detection Systems (IPS / IDS).
- ☑ Limiting access to those who need it only.
- ☑ Written data security policies.
- ☑ Annual security.

emergence