THE HUMAN HACKER

The Layer 8 Security monthly newsletter

HINTS AND TIPS

Email and messaging services, including social media platforms, are some of the primary ways we communicate today.

We not only use these technologies every day for work, but also to stay in touch with friends and family.

Since so many people around the world depend on these technologies, they have become one of the primary attack methods used by cyber attackers.

This attack method is called phishing.

WHAT IS PHISHING?

Phishing is a type of attack that uses email or a messaging service to fool you into taking an action, such as clicking on a malicious link, sharing your password, or opening an infected email attachment.

Attackers work hard to make these messages convincing and tap your emotional triggers, such as urgency or curiosity. They can make them look like they came from someone you know, such as a friend or a trusted company you frequently use.

Attackers then send these messages to millions of people. They do not know who will take the bait, all they know is the more they send, the more people will fall victim to the attack.

In this newsletter:

w: www.layer8security.com.au
e: information@layer8security.com.au
p: 1300 536 706

PROTECTING YOURSELF

In almost all cases, opening and reading an email or message is fine. For a phishing attack to work, the bad guys need to trick you into doing something. Fortunately, there are clues that a message is an attack. Here are the most common ones:

- Pressuring you to bypass or ignore your policies or procedures at work.
- A strong sense of curiosity or something that is too good to be true (no, you did not win the lottery).
- Requesting highly sensitive information, such as your credit card number, password, or any other information that a legitimate sender should already know.
- You receive a message from someone you know, but the tone or wording does not sound like him or her. If you are suspicious, call the sender to verify they sent it. It is easy for a cyber attacker to create a message that appears to be from a friend or coworker.
- A generic salutation like "Dear Customer". Most companies or friends contacting you, know your name.
- The message says it comes from an official organisation but has poor grammar or spelling or uses a personal email address like @gmail.com.
- A tremendous sense of urgency that demands "immediate action" before something bad happens, like threatening to close an account or send you to jail. The attacker wants to rush you into making a mistake.

'If an email or message seems odd, suspicious or too good to be true, it may be a phishing attack'

THE 4 TRIGGER RULES

- Does the email have a "link" to click?
- Does the email have something to download?
- Is the email asking for confidential information?
- Does the sender want you to undertake an action, like send money?

If the answer is YES, put the email aside for a more in-depth investigation