insight

Social Engineering

Keep your data safe from these cyber attacks

Social engineering in cyber security is the psychological manipulation of people into performing actions or divulging confidential information. Candidates for a social engineering attack can range from a corporate executive to an elementary school student. Even the most seasoned IT professional can be victimized by this type of attack.

98%

98% of cyber attacks rely on **social engineering.**

New employees are the most susceptible to socially engineered attacks, with 60% of IT professionals citing recent hires as being at high risk.

Social engineering occurs in three stages:

1. **Research**
The research stage is one of the crucial phases in the planning of a cyber-attack. Hackers will often gather information for several weeks or months before implementing their attack.

2. **Planning**
Using the information they gathered, the attacker selects their mode of attack and designs the strategy and specific messages they will use to exploit the target individuals' weaknesses.

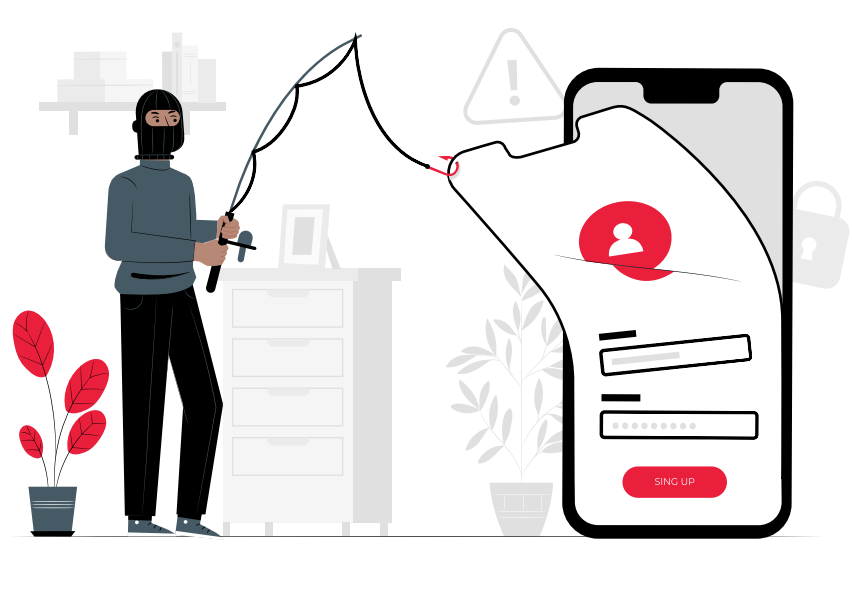
3. **Execution**
The attacker carries out the attack usually by sending messages by email or another online channel. Once this happens, they can then jeopardise the organisations systems and software.

Phishing

Recognize and avoid phising scams

What is Phishing?

Phishing refers to an attack that is usually sent in the form of a link embedded within an email. The email is disguised and looks like an email from a reliable source, but in reality, it's a link to a malicious site.



30%

30% of phishing messages get opened by targeted users.

12%

12% of those users click on the malicious attachment or link.

How to protect yourself against it

1. **Always update your computer and mobile software.** Set the software to update automatically

2. **Use multi-factor authentication.** It makes stealing your information harder for cyber criminals.

3. **Backup your data.** Creating backups is a critical step in computer maintenance to protect your data in the event of system failure or file corruption.

Vishing

(Voice Phishing)

What is it?

Vishing attempts to trick victims into giving up sensitive information over the phone. In most cases, the attacker strategically manipulates human emotions, such as fear, sympathy, and greed in order to accomplish their goals.

37%

Vishing, has a success rate of 37%

75%

This increases to 75% when combined with email phishing.

How to protect yourself against it

- Don't answer calls **from numbers you don't recognize.**
- Do not give any caller **personal or company Information.**
- **Be wary of a phone call claiming to be from a government agency** or bank asking you for sensitive information or money.
- **Never trust anyone who creates urgency** and convince you to call right back.

Smishing

(SMS Phishing)

What is it?

Smishing is a cyber attack that uses SMS text messages to mislead its victims into providing sensitive information to a cybercriminal. The text message might ask the victim to confirm delivery of an Amazon order or ask the recipient to click a link to finish registering in a new government program.

Smishing attacks have risen 328% in 2020 alone.

How to protect yourself against it

Smishing attacks can steal user information using fake two-factor authentication (2FA) messages.

- **Treat all 'you must act immediately' messages suspiciously.**
- **Do not click links sent to you via text message.**
- **Make sure you deploy comprehensive mobile security** to protect your phone from hacking attempts.
- **Your banks or any other financial institution will not ask for sensitive information** or to click on a link to share account credentials.

Watering Hole

What is a Watering Hole?

Much like phishing, a watering hole attack is used to distribute malware onto victims' computers. Cybercriminals infect popular websites with malware. If anyone visits the site, their computers will automatically be loaded with malware.

This style of attack is so effective that Microsoft, Apple, Facebook, and Twitter have all fallen victim to it.

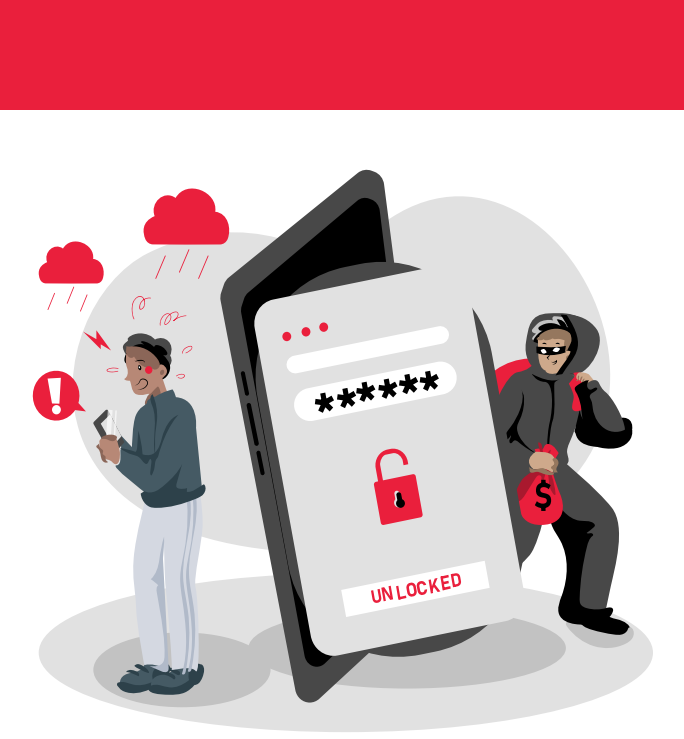
How to protect yourself against it

- **Update your software.**
- **Hide your online activities with a VPN.**
- **Regularly conduct security checks using your network security tools.**

Pretexting

What is Pretexting?

An attacker can impersonate an external IT services operator to ask internal staff for information that could allow accessing system within the organization. In these types of attacks, the scammer usually says they need certain bits of information from their target to confirm their identity.



How to protect yourself against it

- **Establish security protocols,** policies, and procedures for handling sensitive information.
- **Do not divulge sensitive information** to unverified entities via email, phone, or text messages.
- **Be wary of offers that seem "too good to be true".**

93%

Phishing and pretexting are responsible for 93% of successful data breaches.

Whaling Attacks

What is a Whaling Attacks?

Whales – or company executives – are the biggest fish in the sea. **Whaling attack targets a specific executive or senior employee with the purpose of stealing money or information,** or gaining access to the person's computer in order to execute further cyberattacks.

Attackers are attempting to make the email look as if it is an internal email by changing a letter like "I" to a number "1".

What can you do?

- **Educating top officials** about phishing attack whaling is the best way to pre-emptively defend against such attacks.
- **Never click unknown links or download attachments.**
- **Install security software** to defend against whale phishing.
- **Security training programs for employees.**

Tailgating

What is Tailgating?

Also known as "piggybacking", tailgating is the physical act of unauthorized entry of a person following an authorized entrant. The attacker seeks entry to a restricted area that lacks the proper authentication.

80%

80% of cyber-liability claims come from employee negligence, including rogue employees.

Additionally, **ex-employees are often disgruntled,** seeking revenge and damaging property, and stealing company information and sensitive data to enact this revenge.

What can you do?

- **Staff Education:** Explain the risks of tailgating and why staff should never open the door for someone they do not know.
- **Have a reception staff** to help prevent unauthorized persons from entering the building.
- Visitors and temporary employees **should wear identification cards** or badges to indicate they are authorized to be in the building.

Recognizing social engineering attacks will help protect your organization and ensure effective cybersecurity practices. If you need help implementing tighter network controls like stringent firewall settings, end-point protection, and white-listing of websites or applications, **talk to one of our experts at Insight IT.**