

SOCIAL ENGINEERING IN BUSINESS

Social engineering is an act, simple or complex, that influences a person to make a decision that is not in their best interest. Cybercriminals are social engineers. They use their skills to exploit weaknesses not in technical IT infrastructure, but the people using it. People like you, your colleagues, and your business associates.

If a wrong move is made, from downloading a simple attachment, clicking on a URL in an email to a fake money transfer, one IT user can give a hacker free rein of an organisation's IT infrastructure.

This is your essential cheat sheet for identifying and ceasing social engineering, to protect yourself and your colleagues.

“**Every day, IT users can put data and systems at major risk of a social engineering attack. After all, it is easier to hack a single person than a business.**”



PSYCHOLOGICAL CYBER TRIGGERS



Social engineering preys on human behaviour, predicting how we will react to pressure or a proposition. So, it is critical to remain clear headed when using company communications. Treat every email, text, and phone call with vigilance and neutrality. Ideally, take ten before tackling your inbox or responding to unsolicited communications.

THE TOP SOCIAL ENGINEERING ATTACKS

- Phishing:** A generic, malicious email, casting a wide net and hoping somebody bites the bait. Often less sophisticated, but not always easier to spot.
- Whaling:** A targeted attack against a high-value or influential figure in a business. Big fish are often closer to the crown jewels – money and data.
- Vishing:** Fraudulent calls that put pressure on the target to follow through on a request, such as paying a late invoice or providing remote laptop access.
- Smishing:** A fake text often impersonating governments or banks. It trick recipients into tapping unsafe links or revealing sensitive information.
- CEO Scam:** The business email of a high-ranking figure is hacked. Emails are sent impersonating them as a means of obtaining cash.
- Scareware:** Bombards with false cybersecurity alarms, prompting the install of malicious software under the guise of a helpful solution.
- Pretexting:** Inventing a scenario to convince users to divulge information they never would out of context. Fake authority figures are often involved.
- Quid Pro Quo:** Attempts a trade of service for information or access, pretending to be reaching “someone else”, but luring the victim in during conversation.
- Baiting:** Lures victims into providing sensitive information or credentials by promising something of value for free.
- Diversion:** The thief persuades a delivery driver or courier to travel to the wrong location or hand off a parcel to someone other than the intended recipient.
- Honey Trap:** Pretends to be romantically or sexually interested in the victim and lures them into an online relationship.

WARNING CALLS FOR SOCIAL ENGINEERING ATTACKS

Social engineering attacks typically share the same features. The type of attack that a threat actor deploys depends on what a user is most likely to bite on. Think carefully about what this means, and how criminals exploit us. For example:

- Scareware is often deployed after a cyber breach makes headlines
- Pretexting targets organisations with assumed robust cybersecurity
- Vishing can catch remote or field workers off guard
- CEO scams may intensify after government announcements

SPOT SOCIAL ENGINEERING CHECKLIST

- The communication has no named introduction, a generic introduction, or uses your email or phone number.
- The sender's email or ID exactly matches the domain of the organisation, including from safe senders and online. When you long hover, links and email addresses are unclear, unusual, or suspicious, or a website has an uncommon domain and no security certificate.

From: IT Team <012711.service.fp13221@email.com>
To: joe.bloggs@email.com
Subject: Awaiting Payment
Attached: Latest Compliance Documents.zip

Dear joe.bloggs@email.com

Your account needs updating. Click link to update – IT Teams.

Log in

- There is an unsolicited, unexpected, or unnecessary file attachment. The file may be a zip file.
- The communication, spoken or written, has poor grammar and spelling, or unusual phrasing in some way.
- The communication asks for any personal details, including payment or logins.

What should you do? If you spot just one of these warning calls, stop, complete your threat checklist, and contact the IT department immediately. And never click, reply or forward a communication.

COMMON CONTENT THEMES FOR BUSINESS USERS



PLAY THEM AT THEIR OWN GAME!

As an IT user, you are likely to be the first line of defence against cyberattack. But this doesn't have to be high pressure if you follow our tips. Here are 6 steps to outsmarting social engineering threats and reducing the risk of falling in the workplace. **Confirm with IT leaders if these measures are in place.**

- 1 Use an encrypted network and communications
- 2 Attend training sessions and complete simulation tests
- 3 Know how to report a near-miss or worrying message
- 4 Have a named Chief Information Security Officer (CISO) or VCISO
- 5 Check cybersecurity software is installed and updated
- 6 Understand your role in valid cyber insurance

<https://www.clearedin.com/blog/phishing-attack-statistics>
<https://threatcop.com/blog/top-5-cyber-attacks-and-security-breaches-due-to-human-error/>
<https://firewalltimes.com/social-engineering-statistics/>
<https://www.forbes.com/sites/zacharysmith/2022/03/22/cybercriminals-stole-69-billion-in-2021-using-social-engineering-to-break-into-remote-workplaces/>