

CIAL ENGINEERING BUSINESS

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

Social engineering is an act, simple or complex,

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

44

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.

a single business every year

700+

social engineering attacks hit

£6.91 BILLION

is lost annually to social

engineering attacks



of phishing

software

attacks make

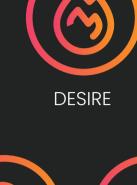
it past security



of cyber breaches

PSYCHOLOGICAL CYBER TRIGGERS







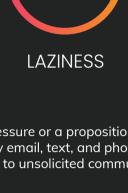




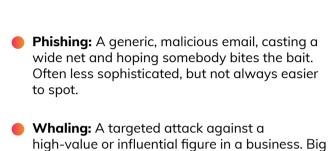








THE TOP SOCIAL



money and data.

information.

alarms, prompting the install of malicious wide net and hoping somebody bites the bait. software under the guise of a helpful solution. Often less sophisticated, but not always easier **Pretexting:** Inventing a scenario to convince Whaling: A targeted attack against a users to divulge information they never would out of context. Fake authority figures are often

involved.

ENGINEERING ATTACKS

laptop access. **Smishing:** A fake text often impersonating governments or banks. It trick recipients into tapping unsafe links or revealing sensitive

Vishing: Fraudulent calls that put pressure on

the target to follow through on a request, such

as paying a late invoice or providing remote

fish are often closer to the crown jewels -

- **CEO Scam:** The business email of a high-ranking figure is hacked. Emails are sent impersonating them as a means of obtaining
- 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:

The communication has no named

uses your email or phone number.

Dear joe.bloggs@email.com

Log in

Failed delivery

or money

Software

installs or

service sign

ups

From:

To:

introduction, a generic introduction, or

joe.bloggs@email.com

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.

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.

The communication, spoken or written, has poor grammar and

spelling, or unusual phrasing in

The communication asks for

any personal details, including

some way.

payment or logins.

information or access, pretending to be

Quid Pro Quo: Attempts a trade of service for

Scareware: Bombards with false cybersecurity

- **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.
- into an online relationship.

Honey Trap: Pretends to be romantically or sexually interested in the victim and lures them

Vishing can catch remote or field workers off guard

CEO scams may intensify after government announcements

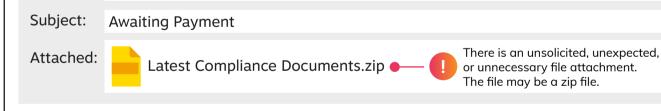
SPOT SOCIAL ENGINEERING

Pretexting targets organisations with assumed robust cybersecurity

Scareware is often deployed after a cyber breach makes headlines

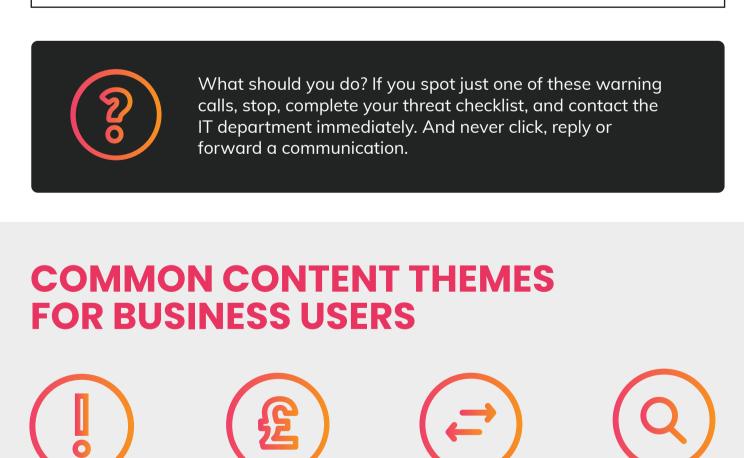
WARNING CALLS FOR SOCIAL ENGINEERING ATTACKS

CHECKLIST The sender's email or ID exactly matches the domain of the



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

IT Team <012711.service.fp13221@email.com



payment account credit account access top-up

Identification

verification to access

services

Invoice

payments or



File sharing or

business

You've been

victim of a

cyberattack



Password

resets or

suspicious

activity

A favour, such

as providing a

password

Use an encrypted network and communications

Know how to report a near-miss or worrying message

Attend training sessions and complete simulation tests

Have a named Chief Information Security Officer (CISO) or VCISO

Understand your role in valid cyber insurance

Check cybersecurity software is installed and updated

https://www.forbes.com/sites/zacharysmith/2022/03/22/cybercriminals-stole-69-billion-in-2021-using-social-engineering-to-break-into-remote-workplaces/

https://threatcop.com/blog/top-5-cyber-attacks-and-security-breaches-due-to-human-error/https://firewalltimes.com/social-engineering-statistics/

https://www.clearedin.com/blog/phishing-attack-statistics