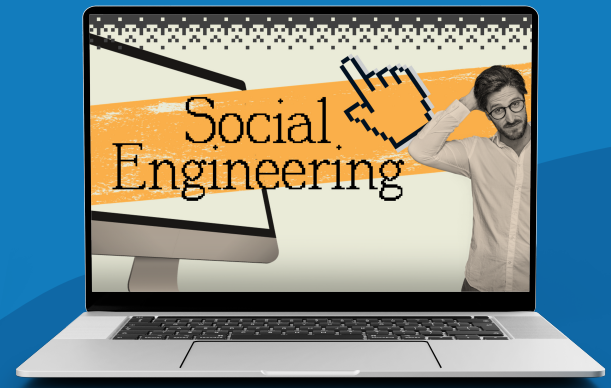


Social Engineering

If you got an urgent email from your boss asking for your company's latest financial reports, what would you do? Cybercriminals can pretend to be your coworkers, using only public information, sending you emails and asking for things; if you're not careful, you might not catch the difference. This is called "social engineering," and it can have major consequences.



Key takeaways:

- Social engineering is a tactic used by attackers to manipulate people into divulging sensitive information or performing certain actions. For instance, it could be someone posing as IT support asking for your password to do required maintenance on your computer.
- When you receive a suspicious message asking for private data, even if you know the sender, it's best to contact them directly to confirm the authenticity of the message.
- It's more than OK to say no to giving that stranger access to your computer or sending them company files until you have confirmation from someone you know and trust.

Glossary:

Here's a quick refresher on the most common social engineering strategies:

▶ **Phishing** – using email, text messages, phone calls, or social media posts to spread malware or trick you into providing sensitive data

▶ **Pretexting** – tricking you into providing access to sensitive information by presenting a credible story and pretending to be someone you can trust

▶ **Baiting** – enticing you into accidentally compromising your security

▶ **Quid Pro Quo** – explicitly offering you something of value, often in the form of a service, in exchange for sensitive information

▶ **Diversion Theft** – stealing confidential information by convincing you to send it to the wrong recipient

Reflection:

Have you received any suspicious emails, texts, or phone calls recently? What did you notice about them that rang an alarm, and what did you do about it? Attackers will take advantage of the complacency that comes along with routine, so it's important to make vigilance a part of your routine.