CICADA | RESOURCES

LESSON 01 OF 04 · 6 MIN · ESSENTIAL

How social engineering works

Most scams don't hack software. They use urgency, authority and trust to make a normal person do something unusual.

Attack the person, not the system

Social engineering is persuasion with a criminal purpose. It works because the request is plausible and the moment is busy. The attacker doesn't need to break encryption if someone will read out a code, approve a payment or click a link.

Four levers do most of the work: **urgency** (“before close of business”), **authority** (“the director asked”), **trust** (a familiar supplier, a real email thread) and **secrecy** (“don't tell anyone yet”).

The tell is the process, not the spelling

Modern scam emails are well written and may come from a real, compromised mailbox. Looking for typos is unreliable. Instead, notice when a request steps outside the normal process: new bank details, a payment to a personal account, a code read aloud, a login from a link, a change of payroll destination.

Legitimate urgency exists. Legitimate secrecy around money usually doesn't.

A protocol that beats it

Agree one rule: **any request involving money, access or credentials is verified on a second channel**, using a number or address you already hold. Not a reply, not a number in the message. Then make it safe to slow down: no blame for reporting, and a named person to call.

> THE PAUSE

> Almost every scam depends on you not pausing. A 30-second gap, “I'll call you back on the number I have”, breaks the spell and often ends the attack.

Key takeaways

- ✓ Scams target people and process, not just software.
- ✓ Urgency, authority, trust and secrecy are the four levers.
- ✓ Well-written emails can come from real compromised accounts.
- ✓ Verify money and access requests on a second channel.