CYBERSECURITY 101 · eBuilder Security

Social Engineering

Most attacks now start with a person, not a system. Here is what your team is up against and the one habit that stops it working.

WHAT IT IS

Social engineering is the manipulation of people into handing over access, information or money. Instead of breaking into a system, the attacker persuades someone who already has legitimate access to act for them. It arrives as an email, a phone call, a text message or a visitor at reception, and it works because the request looks routine. Phishing, vishing, CEO fraud and help desk impersonation are all versions of the same move.

WHY IT MATTERS

About 60%

Of observed initial access cases in the EU involved phishing in some form, ahead of vulnerability exploitation at 21.3%.

ENISA Threat Landscape 2025

75.2%

Of the 33,514 attempted frauds reported to the Swedish Police in 2025 were attempted vishing.

Polismyndigheten, April 2026

1.7 points

The average failure-rate gap between trained and untrained staff in a trial of 19,500 employees.

IEEE Security and Privacy, 2025

WHAT HAPPENED

In April 2025 attackers impersonated an employee to an outsourced IT service desk and obtained a password reset at Marks and Spencer. The retailer's chairman told a UK parliamentary committee that entry happened on 17 April through what he called a sophisticated impersonation, with a third party involved at the point of entry. The company told investors the incident would cost roughly 300 million pounds in operating profit before mitigation, and online ordering stayed down for about six weeks.

RED FLAGS TO WATCH FOR

Spelling mistakes are no longer the giveaway. Watch the behaviour around the request.

- A deadline that only the sender set.
- Secrecy, or a claim that the normal approver is unavailable.
- A move to a channel with less verification, such as a mobile number or a chat app.
- Bank details, a payroll account or a delivery address that must change today.
- An MFA prompt you did not trigger, or several in a row.
- Resistance to a callback on a number you already hold.

THE ONE RULE THAT STOPS IT

Before you move money or change access, verify the request on a channel you chose yourself, using contact details you already hold.

THEN BUILD THE HABIT AROUND IT

- Call back on the number in your own directory, never the one in the request.
- Require two approvers above a payment threshold you set.
- Give the help desk an identity check that does not rely on details an attacker can look up.
- Hold outsourced service desks to the same standard in the contract.
- Report a mistake immediately. The response window is measured in minutes.

MYTHS AND FACTS

MYTH

Our staff have done the training, so we are covered.

FACT

A randomised trial of more than 19,500 employees published at IEEE Security and Privacy in 2025 found no significant link between recent annual training and failing a phishing simulation.

MYTH

Multi-factor authentication stops it.

FACT

Push bombing, SIM swapping and help desk factor resets all defeat ordinary MFA. The FBI and CISA recommend phishing-resistant MFA using FIDO or WebAuthn.

MYTH

A live video call proves who you are talking to.

FACT

At Arup in January 2024 a finance employee joined a call with the CFO and colleagues, all of whom were AI recreations, and sent HK$200 million in 15 payments.

THE LEGAL DUTY

Security awareness training is a legal duty under NIS2 Article 21.2g, in force in Sweden as Cybersäkerhetslagen (SFS 2025:1506) since 15 January 2026. Boards are personally accountable under Article 20, and a significant incident needs an early warning to MCF (formerly MSB) within 24 hours.

GET HELP

eBuilder Security is a Swedish security provider running security awareness training, phishing simulation and social engineering testing that build exactly this verification habit. Read the full guide at the link below.

Read the Full Article →