CYBERSECURITY 101 · eBuilder Security

Security Awareness Training

Most breaches now turn on a person, not a firewall. Here is what security awareness training is, what the evidence says actually works and the one habit that stops the attacks aimed at your team.

WHAT IT IS

Security awareness training teaches your people to recognise and safely handle the attacks aimed at them, from phishing and vishing to invoice fraud and help-desk pretexting. It matters because attackers target people, not just systems. Done well it changes behaviour and builds a reporting habit. Done as a once-a-year video it barely moves the numbers, which is why how you run it matters as much as whether you run it.

WHY IT MATTERS

62%

Of breaches involve the human element, making people the most attacked layer in any organisation.

Verizon 2026 DBIR

$2.77 billion

Business email compromise losses reported to the FBI in the US in 2024.

FBI IC3, 2025

about 19%

Drop in susceptibility when staff complete interactive training. Training as usually run cut the click rate by only about two percentage points.

UC San Diego, 2025

WHAT HAPPENED

In September 2023 attackers phoned the MGM Resorts IT help desk, posed as an employee and talked their way past identity checks to reset access. The intrusion became a ransomware attack that disrupted hotels and casinos for around ten days and cost the company roughly 100 million dollars. No one was fooled by a bad email. The weak point was a help desk with no reliable way to prove who was calling. (MGM Resorts SEC filing, 2023)

RED FLAGS TO WATCH FOR

You cannot reliably spot a modern attack by eye, so watch the behaviour, not the polish.

- Urgency and secrecy, a request that supposedly cannot wait or go through normal channels.
- A caller claiming to be IT or a colleague and asking for a password or an MFA approval.
- Any request to change supplier or payroll bank details.
- Pressure to skip the usual payment or sign-off process.
- Contact through an unusual channel, like a surprise call, text or QR code.

THE ONE RULE THAT STOPS IT

Verify any unusual request for money, access or credentials through a second known channel before you act. Never through the channel the request arrived on.

THEN BUILD THE HABIT AROUND IT

- Run short, frequent, interactive training that people actually finish, not one annual module.
- Reward reporting and never punish an honest mistake, so a click becomes an alert in minutes.
- Require a second out-of-band check for any payment or change of bank details.
- Give the help desk an identity test a caller cannot fake.
- Deploy phishing-resistant multi-factor authentication so a stolen password is not enough.

MYTHS AND FACTS

MYTH

Security awareness training stops phishing on its own.

FACT

A 2025 University of California, San Diego trial of 19,500 staff found training as usually run barely changed the click rate. It works only as one layer among technical controls.

MYTH

One training session a year is enough.

FACT

A single annual module is forgotten within weeks. Short, frequent and interactive training that people complete is what changes behaviour.

MYTH

Only junior or non-technical staff need training.

FACT

Executives and finance approvers are prime targets because they authorise money and access. Under NIS2 the board is personally accountable for security.

THE LEGAL DUTY

Security awareness training is now a legal duty under NIS2, in force in Sweden as Cybersäkerhetslagen since 15 January 2026, with boards personally accountable under Article 20. DORA, GDPR and ISO 27001 all carry the same expectation.

GET HELP

eBuilder Security builds and runs Sweden-based security awareness training on exactly this model, short enough that people finish it and backed by the reporting culture and technical controls that catch what training misses. Read the full guide at the link below.

Read the Full Article →