CYBERSECURITY 101 · EBUILDER SECURITY

Phishing

Phishing is still how most attackers get in, and the badly spelled email you were trained to spot is a decade out of date. Here is what your team needs to know, and the one habit that stops it.

WHAT IT IS

Phishing is a fraud in which an attacker sends a message that looks like it comes from someone you trust, such as your bank, a supplier or your own IT department, to trick you into handing over a password, approving a payment or opening a file that installs malware. It arrives by email, SMS, phone call or QR code. It is not a nuisance for the IT team to filter. It is the front door.

WHY IT MATTERS

60 percent

Of observed intrusions in Europe started with phishing, making it the leading way in.

ENISA Threat Landscape 2025

215.8 million dollars

Reported phishing losses in 2025, more than triple the 2024 figure even though attack volume stayed flat.

FBI IC3, 2025

75.2 percent

Of attempted frauds reported to the Swedish police in 2025 were vishing, made by phone.

Polismyndigheten, 2025

WHAT HAPPENED

In April 2025 someone phoned a help desk, posed as a Marks and Spencer employee and had that account's credentials reset. The retailer's chairman later told a UK parliamentary committee that this impersonation was the point of entry. Online orders stopped for weeks and the company put the damage at around 300 million pounds of operating profit. No malware was needed. A convincing voice was enough. (UK Parliament, Business and Trade Sub-Committee, July 2025)

RED FLAGS TO WATCH FOR

The spelling and grammar tells are gone, so watch the behaviour instead of the wording.

- Urgency or a threat. Act now, or the account closes.
- Secrecy. A deal or a payment you must not discuss with anyone.
- A request that skips the normal process, or arrives through an unusual channel.
- Any change to bank details, payment routes or payroll destinations.
- An attachment you were not expecting, even from someone you know well.
- A caller who resists being called back on a number you already hold.
- A login page your password manager refuses to autofill. The domain is wrong.

> THE ONE RULE THAT STOPS IT
>
> **Verify every unusual or money-related request through a second channel you already trust. Never through the channel the request arrived on.**

THEN BUILD THE HABIT AROUND IT

- Confirm supplier bank-detail changes by calling a number you already hold.
- Require two people to authorise payments above a set amount.
- Give the help desk an identity check that does not accept a confident voice as proof.
- Move administrators to phishing-resistant multi-factor authentication, meaning FIDO2, WebAuthn or PKI.
- Make reporting one click, and never punish anyone for clicking.

MYTHS AND FACTS

MYTH You can spot a phishing email if you look closely enough.

FACT The UK's NCSC says no training package can teach people to catch every attempt. AI has already removed the spelling mistakes staff were taught to look for.

MYTH We have multi-factor authentication, so phishing cannot hurt us.

FACT CISA warns that SMS codes and push prompts can be relayed through a fake login page or bombarded until someone approves. Only phishing-resistant MFA is bound to the real domain.

MYTH Phishing is an email problem.

FACT Of the 33,516 attempted frauds reported to the Swedish police in 2025, 25,199 were vishing attempts, made by phone. QR codes, SMS and help desk calls carry the same attack.

THE LEGAL DUTY

Security awareness training is now a legal duty under NIS2, in force in Sweden as Cybersäkerhetslagen (SFS 2025:1506) since 15 January 2026, with boards personally accountable under Article 20.

GET HELP

eBuilder Security runs security awareness training for organisations in Sweden, built around verification habits rather than click rates. Read the full guide at the link below.

ebuildersecurity.com/cybersecurity-101/phishing

eBuilder Sweden AB · Kista, Stockholm · Cybersecurity 101 series