CYBERSECURITY 101 · eBuilder Security

Vishing

Vishing is voice phishing, a phone call that talks a member of staff into handing over a login, a code or a payment. Here is what your team needs to know and the one habit that stops it.

WHAT IT IS

Vishing, or voice phishing, is a social engineering attack carried out by phone. A criminal impersonates someone the target trusts, often IT support, a bank or a senior colleague, and uses a believable story and pressure to extract a password or one-time code, an approval or a payment. It is no longer just a consumer scam. The same technique now breaks into companies, often by phoning the IT help desk, and cheap AI voice cloning has made the calls harder to doubt.

WHY IT MATTERS

193,407

Phishing and spoofing complaints to the FBI in 2024, the family that includes voice phishing and the most reported cybercrime type in the US.

FBI IC3, 2024

About 100 million dollars

The hit to MGM Resorts' quarterly results after a single help-desk vishing call in 2023.

MGM Resorts, 2023

About 15 million dollars

Cryptocurrency losses reporting linked to the Retool vishing breach in 2023.

CoinDesk, 2023

WHAT HAPPENED

In September 2023 the Scattered Spider group found an MGM Resorts employee on LinkedIn and phoned the company's IT help desk to reset an account. That single call led to administrative access, ALPHV ransomware and about ten days of disruption across MGM's casinos and hotels. MGM later told investors the attack cut about 100 million dollars from one quarter. (CISA and FBI, 2023)

RED FLAGS TO WATCH FOR

You cannot trust caller ID and you cannot reliably hear a fake voice, so watch the behaviour of the call.

- Urgency and secrecy, a request that supposedly cannot wait.
- Pressure to skip a normal payment or sign-off step.
- A push to move to an unusual channel like WhatsApp or Signal.
- Any ask for a password, a one-time code or a payment by phone.
- Reluctance to let you hang up and call back on a known number.

THE ONE RULE THAT STOPS IT

Before acting on any unusual or high-value request, verify it on a second channel you contact yourself.

THEN BUILD THE HABIT AROUND IT

- Require two people to authorise large payments and any change of bank details.
- Give the IT help desk a strict identity check before any password or MFA reset.
- Never read a one-time code to a caller, and use phishing-resistant hardware keys.
- Agree a code word for sensitive requests inside your team.

MYTHS AND FACTS

MYTH

I would recognise a fake voice.

FACT

You probably would not. Cheap tools clone a familiar voice from a short clip, and the FBI warns they can sound nearly identical to a real contact.

MYTH

Caller ID proves who is calling.

FACT

It does not. Attackers routinely spoof numbers so a call looks like your bank, a colleague or an internal line.

MYTH

Multi-factor authentication stops vishing.

FACT

Not on its own. Vishing talks people into reading out the code. Phishing-resistant hardware keys are the reliable backstop.

THE LEGAL DUTY

Security awareness training is a legal duty under NIS2, in force in Sweden as Cybersäkerhetslagen since 15 January 2026, with boards personally accountable under Article 20.

GET HELP

eBuilder Security runs Sweden-based security awareness and phishing-simulation training that builds exactly this verification habit. Read the full guide at the link below.

Read the Full Article →