

# Human Firewall

Your people are the most targeted part of your organisation. A human firewall turns them into a line of defence that stops what technology lets through.

## WHAT IT IS

A human firewall is the layer of defence formed by trained, security-aware staff. They recognise social engineering, pause on unusual requests, verify them through a known channel and report anything suspicious. It covers the judgement calls software cannot make for you.

## WHY IT MATTERS

**62%**

of breaches involved the human element

Verizon DBIR, 2026

**2.77 billion dollars**

reported BEC losses across 21,442 complaints

FBI IC3, 2024

**about 100 million dollars**

MGM Resorts quarterly impact from one help desk call

MGM SEC filing, 2023

## WHAT HAPPENED

In September 2023 attackers looked up an MGM Resorts employee on LinkedIn, then phoned the IT help desk posing as that person and asked for a password and MFA reset. The help desk complied, ransomware followed and MGM reported a roughly 100 million dollar impact for the quarter. Sources: MGM SEC filing and a joint CISA and FBI advisory.

## RED FLAGS TO WATCH FOR

**Most social engineering shares the same tells.**

- Urgency and pressure to act before you can check
- A request that leans on a senior name or outside authority
- An unusual channel, or an out-of-the-blue change of bank details
- A display name or domain that does not quite match
- Being told to keep the request quiet or skip the normal process

## THE ONE RULE THAT STOPS IT

**Verify any urgent or unusual request through a second, known channel before you act, and never use the contact details in the message itself.**

## THEN BUILD THE HABIT AROUND IT

- Report suspected phishing straight away, as a one-click, no-blame action

- Verify identity at the help desk before any password or MFA reset
- Enforce phishing-resistant multi-factor authentication on email, VPN and admin tools
- Practise with regular phishing simulations and track the report rate

## MYTHS AND FACTS

### MYTH

Good technology makes a human firewall unnecessary.

### FACT

Attackers target people because they bypass technical controls. The human element featured in 62% of breaches in Verizon's 2026 report.

### MYTH

Training eliminates clicking.

### FACT

Verizon found the click rate was largely unaffected by training. The real gain is faster reporting, which shrinks the attacker's window.

### MYTH

Only careless or junior staff get fooled.

### FACT

Finance teams, IT help desks and executives are prime targets. The Google and Facebook fraud tricked finance staff at two highly technical firms.

## THE LEGAL DUTY

NIS2 and the Swedish Cybersäkerhetslagen (SFS 2025:1506, in force 15 January 2026) make security awareness training a required measure and a board-level duty, with fines up to 10 million euro or 2% of global turnover for essential entities.

## GET HELP

**eBuilder Security runs Sweden-based security awareness training and phishing simulations that build exactly these habits. Read the full guide at the link below.**

[Read the Full Article →](#)