THREATS LIBRARY

JULITH GmbH
Awareness-as-a-Service

Recognise & stop phishing — the complete guide

94% of all successful cyber attacks start with a phishing email. Here is how to unmask them in three seconds — and what to do when someone has already clicked.

min read: 9 min **Updated:** 14 March 2026 **Risk:** Very high risk
Source: awareness-as-a-service.com/en/resources/threats/phishing

What is phishing?

Phishing is the attempt to trick you into revealing credentials, payment information, or taking harmful actions — most commonly via email, and increasingly via SMS (`Smishing`), QR code (`Quishing`), or phone call (`Vishing`).

Unlike technical attacks, phishing targets people directly. It exploits psychological levers: time pressure, authority, curiosity, fear. That is precisely why technical controls fail regularly — and awareness is the most effective line of defence.

At a glance

01
Most common attack type
94% of incidents start with phishing — especially Business Email Compromise (BEC).

02
11 minutes to click
Average time between receiving and clicking a phishing link. Systems — not just the SOC — must be ready to respond.

03
3 seconds to detect
Sender, salutation, link preview — a 3-second check is enough in 80% of cases.

How do you recognise phishing?

Six warning signs that — alone or combined — indicate phishing:

! **Artificial urgency**
"Within 24 hours", "final notice", "account will be suspended".

! **Callback request**
"Please call this number immediately: +44..." — vishing chain-link.

! **Suspicious domain**
`microsoft-365.support` instead of `microsoft.com`, typos, Unicode tricks.

Impersonal salutation
"Dear customer", even though the sender is supposed to know you.

Unsolicited attachments
Office documents with macros, ZIP archives, HTML files — especially critical.

Suspicious links
Hover preview does not match the visible link, or link via URL shortener.

How to protect yourself

For employees

- 3-second check before every click: sender, domain, link preview.
- When in doubt: **verify via a known channel** (phone, chat) — do not reply to the email.
- Forward suspicious emails using the "Report phishing" button — do not delete them.
- Never enter credentials or MFA codes on pages linked from email.

For administrators

- Configure SPF, DKIM, DMARC (`p=reject`) for all outgoing domains.
- Enable external email banners in Outlook / Gmail Workspace.
- Deploy a "Report phishing" button (e.g. via add-in) — direct channel to SOC.
- Enforce MFA — prefer phishing-resistant methods (FIDO2, passkeys).
- Run quarterly phishing simulations with a learning moment on click.

Real examples

CASE 01 · MID-SIZE MACHINE MANUFACTURER · DE · Q2/2025

A supposed Microsoft 365 email asked to "verify the mailbox". An accountant clicked the link and entered credentials and an MFA code. **Within 90 minutes**, attackers sent a fake invoice to a supplier — using the genuine mailbox.

Damage: EUR 38,000 · **Detection:** 4 days later via a bank query · **Lesson:** Phishing-resistant MFA would have stopped the attack.

CASE 02 · MUNICIPAL ADMINISTRATION · CH · Q4/2025

QR code on a printed "security letter" at reception. Staff scanned it and landed on a fake single sign-on page. The attacker had previously used public press releases to collect employee names.

Damage: no data exfiltration · **Detection:** an attentive IT manager · **Lesson:** include quishing awareness in standard modules.

What to do if it happens?

THE FIRST 15 MINUTES

1. **Stay calm, do not delete.** The email is evidence.
2. **Report immediately:** IT helpdesk / SOC / CISO. No "wait and see" reflexes.
3. **Disconnect from the network** if an attachment was opened or credentials were entered.
4. **Change password immediately** (from a different device). If SSO: invalidate sessions.
5. **Check MFA devices:** were additional devices registered without your consent?
6. **Notify finance / accounting** if payment data may have been exfiltrated.

Frequently asked questions

What is the difference between phishing and spear phishing?

Phishing is sent in bulk. Spear phishing targets specific individuals with researched details (role, projects, personal contacts). Whaling is spear phishing aimed at executives. The protective measures are similar — but the detection threshold for spear phishing is higher.

Can my spam filter detect phishing?

Partially. Bulk phishing is often filtered. BEC and spear phishing are technically inconspicuous — they arrive via real (compromised) accounts, without attachments, without suspicious links. That is precisely why awareness and procedural controls are essential.

Are phishing simulations legally problematic?

They are permissible in Switzerland and Germany, provided the works council / staff representatives are informed and the measure is not used for individual performance monitoring. We supply template agreements for CH (OR), DE (BetrVG), and AT.

What does a successful phishing attack cost on average?

EUR 4.5 million in the DACH region (IBM 2025). Direct damages (wire transfers, ransom) account for about one third — the rest is forensics, downtime, reputational damage, and regulatory consequences.

Related topics

These threats often go hand in hand — anyone who understands phishing should also know CEO fraud, quishing, and AI-based manipulation.