What is phishing?

Phishing is a social-engineering attack that impersonates a trusted person or brand to trick you into revealing a credential, opening malware, or making a payment. It is the most common way attacks begin, because it targets people rather than patched software. The main variants are spear phishing, whaling, and business email compromise, and the core defenses are multi-factor authentication, email authentication, and a habit of verifying unusual requests.

HOW IT WORKS

01 The main types of phishing

Phishing comes in several forms, mostly defined by how targeted they are and how they are delivered:

- Bulk phishing is the wide net: the same generic message sent to thousands, hoping a few respond.
- Spear phishing is targeted, using real details about you or your company to be convincing.
- Whaling is spear phishing aimed at executives, whose access and authority are worth more.
- Business email compromise (BEC) impersonates a boss or supplier to request money or a change of bank details, often with no malware at all.
- Clone phishing copies a real message you have seen before and swaps in a malicious link.
- Smishing and vishing move the attack to text messages and phone calls.

02 Business email compromise: the costly one

The most expensive phishing rarely involves malware. In business email compromise, an attacker poses as your CEO, a supplier, or a partner and simply asks to move money or change the bank details on an invoice. There is nothing for antivirus to catch, because the only payload is a convincing request.

The defense is a process, not a product: any request to move money or change payment details is confirmed on a second channel, a phone call to a known number, never by replying to the email. That single rule stops most BEC losses.

HOW TO DEFEND

- Multi-factor authentication so a stolen password is not enough. Phishing-resistant methods (passkeys or hardware keys) also defeat the real-time proxy attacks that steal one-time codes.
- Email authentication (SPF, DKIM, and DMARC) so attackers cannot spoof your own domain.
- Your provider's advanced anti-phishing, which is often turned down by default.
- Training and simulations so people recognise the signs, and a one-click report button.
- A second-channel rule for any request to move money.

SOURCES

[1] Phishing (Technique T1566)

[2] Avoiding Social Engineering and Phishing Attacks

[3] Data Breach Investigations Report

03 How to spot a phishing attempt

Most phishing gives itself away if you slow down:

- The sender name looks right but the actual address or domain does not.
- It creates urgency or a threat to make you act without thinking.
- It asks for a password, a payment, or an unexpected attachment.
- Links do not match where they claim to go (hover before you click).
- The tone or request is slightly off for the person it claims to be from.

When something feels wrong, the safe move is to stop and verify through a channel you already trust.

See what a successful phishing click would actually reach.

securelayer7.net/learn/threats/phishing

Open online