Checklist: 10 signs of a phishing email

Phishing is a social engineering attack where a threat actor (also known as a cyber criminal) poses as a trusted person or organization to steal sensitive information or gain access to a network. Delivered via email, text, or phone, phishing can lead to breaches, data loss, identity theft, malware, or ransomware.

Since over 3 billion phishing emails are sent every day, you, as well as your family and friends need to know how to recognize phishing emails and take appropriate action to protect yourself and your organization from attack. In this article, we'll cover 10 signs of a phishing attack, what to do if you suspect a phishing email, and how to improve your email defenses.

What is a phishing email?

Like an actual fisherman, an email phisher casts a wide net, sending many emails in hopes that some victims will get caught in their scam.

The term phishing was coined in the mid-1990s. Since then, the rise of AI-generated content, deepfakes (realistic fake photos, audio, and video), and spoofed domains (fake email or website) has made it harder to identify fraudulent emails than ever.

This basic concept has evolved into several types of phishing attacks:

- **Spear phishing:** This is an attack aimed at a specific person or group. Attackers often research personal or job-related details, like financial documents or project names, to design emails that appear legitimate.
- **Whaling:** This phishing attempt targets high-level executives or officials. Using social engineering and personalized details, attackers pose as trusted contacts to steal sensitive data, money, or system access.
- **Clone phishing:** This phishing scam replicates a legitimate email but swaps attachments or links with malicious ones, often from a slightly altered sender address. The goal is to trick recipients into clicking and downloading malware.

Why spotting phishing emails is critical in 2026

Phishing email schemes can be incredibly complex. In 2019, a single bad actor pleaded guilty to stealing over $100 million from both Facebook and Google in a high-level phishing attack that lasted years. The scheme involved fake emails, a fake company, and fake invoices.

Sherwin-Williams, engine parts manufacturer Miba, airliners RyanAir, and several other companies lost millions of dollars to a Russian hacker group that operated by bombarding employees with emails laced with malware attachments.

Damaging phishing scams happen every day, and the stakes aren't just financial loss. Data breaches can cause serious reputational damage and breach of customer trust. The companies mentioned above had some form of cybersecurity before their breaches. Unfortunately, none were enough.

An informed, motivated "human firewall" of educated employees and individuals is the best way to prevent successful phishing attacks and enhance your security posture.

Here is a checklist of the 10 signs of a phishing email with descriptions and guidance below.

- Suspicious sender address or domain
- Urgent or threatening language
- Unexpected attachments or links
- Generic greetings
- Poor grammar or formatting
- Requests for sensitive information
- Mismatched URLs (hover trick)
- Fake login pages or branding inconsistencies
- Odd timing or context
- Too-good-to-be-true offers

Let's cover each of these red flags one by one.

1. Suspicious sender address or domain

Do you recognize the sender address or domain? Is the address littered with strange numbers and names you don't recognize? Ignore the email, clock the email address, and notify the correct authorities.

2. Urgent or threatening language

Intense language that demands immediate action may be a sign of a phishing attack. Email headers like the ones below may be a scam.

- URGENT: Your account will be suspended
- Immediate attention needed
- Final Warning: Your password has been compromised

- Immediate Action Required: Your payment method is invalid
- Payment Failure: Please update your billing information
- Unusual activity detected on your bank account
- Urgent Notice: We have reason to believe your identity has been stolen
- URGENT: Virus detected on your network
- Your email account has been compromised
- Official Notice: Your tax return is being audited

While some legitimate emails may come with urgent language, this kind of language should put you on notice to be cautious and test the email against the other checklist items.

3. Unexpected attachments or links

Don't click on any unexpected attachments or links, especially from senders you don't recognize, and don't forward the email to anyone else.

4. Generic greetings

Generic greetings can be a sign of a bad actor, especially from a source you don't recognize. A new legitimate contact would likely introduce themselves and provide specific, identifying information that ties them to your business, network or someone you know well.

5. Poor grammar or formatting

Misspellings, strange formatting, and poor grammar are signs of a poorly done phishing scam. Fortunately, these messages are easy to catch, report, and block.

6. Requests for sensitive information

Emails that request sensitive information like your credit card number, account number, phone number, and other financial information are a huge red flag. It's best to avoid providing any sensitive information over email; always use an official website instead.

7. Mismatched URLs (hover trick)

Hackers can create a hyperlink that appears legitimate and trustworthy, such as "www.yourbank.com" or "Click here to view your invoice." However, the underlying code for the link points to a completely different, malicious website. This is called a mismatched URL. While most email cybersecurity software is designed to block them, some slip through the cracks.

You can identify mismatched URLs by hovering; when you move your mouse cursor over a hyperlink without clicking, you can see the true, underlying URL, usually in a small pop-up or in the bottom-left corner of the window.

8. Fake login pages or branding inconsistencies

Attackers may send you to fake login pages that look like a website you actually use. Popular pages include PayPal, Venmo, and your bank or retirement accounts.

You can recognize these fake login pages if they have brand inconsistencies or the email contains other phishing red flags.

9. Odd timing or context

An email sent far outside office hours or your normal routine that is unrelated to work (regarding personal life or relating to another industry) may be a sign of a scam. Carefully assess each email you receive to determine whether it's from a coworker in another time zone/personal contact or from a nefarious actor.

10. Too-good-to-be-true offers

If the email seems too good to be true, then it probably is. These email claims are just trying to entice your clicks:

1. You won an award you didn't apply for or that you applied to ages ago
2. You won a large sum of money
3. You got a great new job you didn't apply to or applied to ages ago

What to do if you suspect a phishing email

Don't click, don't reply, and don't forward. Consider this email a potential virtual bomb. Sending it to another employee, family, or a friend increases the chance that the email can cause more damage.

Phishing is the No. 1 email-based threat we all face daily. Security awareness is a skill, not instinct, and confidence comes from practice.

*This information is adapted from information published by AdaptiveSecurity.com