ScamSecurityCheck.com

How to Spot a Phishing Email

6 warning signs that an email is trying to steal your information

Phishing emails give hackers access to your passwords and data.
Learn these 6 signs so you can spot a fake before it's too late.

1 Requesting Sensitive Information

Legitimate companies will never ask for passwords, Social Security numbers, or bank details via email. If an email asks you to 'verify your account' or 'confirm your identity' by providing personal information, it's almost certainly a phishing attempt.

TIP: Real companies handle sensitive info through their secure websites, not email.

2 Lack of Personalization

Real businesses know your name and will address you personally. Generic greetings like 'Dear Customer,' 'Dear User,' or 'Dear Account Holder' are a sign the sender doesn't know who you are — because they're sending this to thousands of people at once.

TIP: If a company you do business with doesn't use your name, be suspicious.

3 Suspicious Links

Hover over any link before clicking it. If the URL doesn't match the company's real website, don't click. Phishers create lookalike URLs like amaz0n-secure.com or paypa1-verify.net to trick you into entering your credentials on a fake site.

TIP: Always type the real website address directly into your browser instead of clicking links.

More Warning Signs

4 Spelling and Grammar Mistakes

Professional companies proofread their emails carefully. Multiple spelling errors, awkward phrasing, or strange formatting are red flags that the email was written by a scammer, often using translation tools or rushing to send thousands of messages.

TIP: Legitimate companies have professional editors. Typos and bad grammar = red flag.

5 Incorrect Sender Address

Always check the actual email address, not just the display name. An email claiming to be from your bank but sent from support@bankk-security-alert.com is a scam. The real company's domain won't have extra words, misspellings, or random numbers.

TIP: Click on the sender name to reveal the full email address. Check it carefully.

6 Unsolicited Attachments

Never open attachments from unknown senders. Legitimate businesses rarely send unexpected attachments. These files can contain malware, ransomware, or viruses that infect your device the moment you open them. Even PDFs and Word docs can be dangerous.

TIP: If you weren't expecting an attachment, don't open it. Contact the sender to verify.

ScamSecurityCheck.com

What To Do If You Receive a Phishing Email

When in Doubt, Don't Click!

Go directly to the company's website by typing the address into your browser.

DO THIS

- ✓ Stop and think before clicking
- ✓ Check the sender's full email address
- ✓ Hover over links to preview the URL
- ✓ Go to the website directly instead
- ✓ Call the company using a trusted number
- ✓ Report the email as phishing/spam
- ✓ Delete the suspicious email
- ✓ Tell a coworker or family member

DON'T DO THIS

- ✗ Click links in suspicious emails
- ✗ Open unexpected attachments
- ✗ Reply with personal information
- ✗ Call numbers listed in the email
- ✗ Forward it to others (report instead)
- ✗ Trust the display name alone
- ✗ Panic — urgency is their weapon
- ✗ Feel embarrassed if you clicked

Scan Suspicious Emails Free at ScamSecurityCheck.com/scanner

Paste any suspicious message and our AI analyzes it for scam patterns.

ScamSecurityCheck.com

Already Clicked? Do This Immediately

1 Disconnect from the internet

Unplug your ethernet cable or turn off Wi-Fi immediately to stop any active data transfer to the attacker.

2 Change your passwords NOW

Start with your email password, then bank, then social media. Use a different device if possible.

3 Run a full antivirus scan

Use your trusted antivirus software to scan your entire device for malware or viruses.

4 Contact your bank

If you entered any financial information, call your bank immediately to freeze your accounts.

5 Enable two-factor authentication

Turn on 2FA for all important accounts so attackers can't log in even with your password.

6 Monitor your accounts for 30 days

Watch for suspicious activity on all accounts. Set up bank alerts for any transactions.

7 Report it

Report to the FTC at reportfraud.ftc.gov and check your breach status at ScamSecurityCheck.com.

Important: We're constantly updating this tool to stay ahead of new and evolving scams. Results aren't guaranteed to be 100% accurate and shouldn't be the only factor in making security decisions. Always trust your judgment.