How to Recognize Phishing

Scammers use email or text messages to try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could get access to your email, bank, or other accounts. Or they could sell your information to other scammers. Scammers launch thousands of phishing attacks like these every day — and they're often successful.

Scammers often update their tactics to keep up with the latest news or trends, but here are some common tactics used in phishing emails or text messages:

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. You might get an unexpected email or text message that looks like it's from a company you know or trust, like a bank or a credit card or utility company. While real companies might communicate with you by email, legitimate companies won't email or text with a link to update your payment information. Or maybe it's from an online payment website or app. The message could be from a scammer, who might

- say they've noticed some suspicious activity or log-in attempts — they haven't
- claim there's a problem with your account or your payment information — there isn't
- say you need to confirm some personal or financial information — you don't
    - Legitimate organizations usually won't ask for sensitive information like passwords, Social Security numbers, or banking details via email.
- include an invoice you don't recognize — it's fake
- want you to click on a link to make a payment — but the link has malware
    - Be very careful when clicking links or opening attachments from unknown or suspicious sources. Hover your mouse over links to see the actual URL before clicking, and avoid opening attachments with suspicious file extensions like ".exe" or ".zip".
- say you're eligible to register for a government refund — it's a scam
- offer a coupon for free stuff — it's not real

- Suspicious Sender: Pay attention to the sender's email address and domain name. Phishing emails often use slightly altered or generic domain names that are similar to legitimate ones.

  Also be on the lookout for these things:

- Generic Greetings: Be cautious if the email addresses you with generic terms like "customer" or "account holder" instead of your name.
- Sense of Urgency: Scammers often try to pressure you into acting quickly by creating a false sense of urgency, like threatening account closure if you don't respond immediately.
- Poor Grammar and Spelling: Emails with numerous errors in grammar, spelling, or sentence structure are often red flags.

How to Report Phishing

If you got a phishing email or text message, report it. The information you give helps fight scammers.

- If you got a phishing **email**, forward it to the Anti-Phishing Working Group at reportphishing@apwg.org.
- If you got a phishing **text message**, forward it to SPAM (7726).
- Report the phishing attempt to the FTC at ReportFraud.ftc.gov.

Sources: TN Comptroller of the Treasury