How To Recognize Phishing/Scam Emails

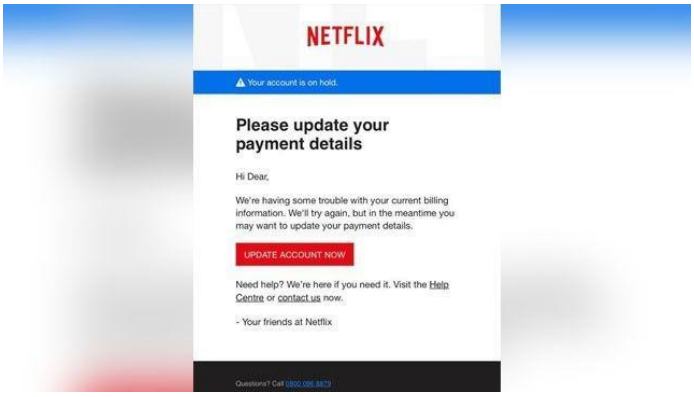
Scammers use email or text messages to try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could get access to your email, bank, or other accounts. Or they could sell your information to other scammers. Scammers launch thousands of phishing attacks 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. 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 payment information — there isn't
- say you need to confirm some personal or financial information — you don't
- 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
- say you're eligible to register for a government refund — it's a scam
- offer a coupon for free stuff — it's not real

Here's a real-world example of a phishing email:
Image



Imagine you saw this in your inbox. At first glance, this email looks real, but it's not. Scammers who send emails like this one are hoping you won't notice it's a fake.

Here are signs that this email is a scam, even though it looks like it comes from a company you know — and even uses the company's logo in the header:

- The email has a generic greeting.
- The email says your account is on hold because of a billing problem.
- The email invites you to click on a link to update your payment details.

While real companies might communicate with you by email, **legitimate companies won't email or text with a link to update your payment information**. Phishing emails can often have real consequences for people who give scammers their information, including identity theft. And they might harm the reputation of the companies they're spoofing.

The email comes from a generic domain (Gmail, Yahoo, etc.)

Generic email domains such as @gmail.com, @yahoo.com, @hotmail.com, and @outlook.com are cybercriminals' favorites for sending scam emails.

These accounts are free to use and can be customized to look like they're coming from a legitimate organization.

A good example is the IRS tax scam [*]. In these scam emails, hackers pretend to be from the IRS and request your SSN to "verify" your identity before they send you a tax refund.

What To Do if You Responded to a Phishing Email

If you think a scammer has your information, like your Social Security, credit card, or bank account number, go to IdentityTheft.gov. There you'll see the specific steps to take based on the information that you lost.

If you think you clicked on a link or opened an attachment that downloaded harmful software, update your computer's security software. Then run a scan and remove anything it identifies as a problem.

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.