RECOGNIZE & REPORT PHISHING SCAMS

WHAT ARE PHISHING SCAMS?

Deceptive messages that mimic trusted sources to trick you into revealing sensitive data or installing malware. Recognizing and reporting these scams is essential to protecting yourself and your organization.

HOW TO SPOT A PHISHING EMAIL

- Too-good-to-be-true offers
  - Free money, prices, luxury items
- Urgent or threatening language
  - “Act now!” “Your account will be deleted!”
- Requests for personal info
  - Passwords or financial data
- Unfamiliar attachments or links
  - Hover to preview URLs
- Mismatched sender addresses
  - Slight misspellings or odd domains
- Poor grammar or generic greetings
  - “Dear Customer”

CAUGHT A PHISHING ATTEMPT?

1. Stay calm. Don’t click or reply
2. Report the email
3. Block the sender
4. Delete the email

APEX technology group

Source: National Cybersecurity Alliance

KNOW THE SCAMMER'S PLAYBOOK: RED FLAGS YOU CAN'T IGNORE

RED FLAGS & WARNING SIGNS

The Danger of Urgency: Scammers use urgency to make you act fast — whether it's a fake prize or a threat.

In phishing messages, a sense of urgency can be negative or positive.

- **Examples of positive sense of urgency:** you won a prize, you're owed money, you can get an exclusive deal.
- **Examples of negative sense of urgency:** You've been hacked, the IRS is investigating you, criminals are recording you through your webcam, there is a warrant out for your arrest.

Requests for sensitive information: Legitimate companies and government agencies will never ask for sensitive personal information, such as your password or Social Security number, via email or text.

Suspicious sender addresses or links: Always check the sender's full email address and hover over any embedded links to see the actual URL. Be cautious of domains that are misspelled (e.g., "amazan.com") or use public domains like "@gmail.com".

Unexpected attachments: Avoid opening unsolicited or unexpected attachments, especially from unknown senders. These can contain malware.

APEX technology group

Source: National Cybersecurity Alliance

KNOW THE SCAMMER'S PLAYBOOK: RED FLAGS YOU CAN'T IGNORE

TYPES OF SCAMS OR THREATS

Spear-Phishing

Some phishing emails are personalized using your name, job, or contacts. These are harder to spot but just as dangerous.

Smishing

Phishing that is carried out through SMS text messages.

Vishing

Phishing that uses voice communication, typically a phone call, to deceive victims.

Spoofing

When an attacker impersonates a legitimate person, website, or email address to deceive a victim.

Pharming

A type of cyberattack that redirects users from a legitimate website to a fraudulent one without their knowledge.

Baiting

An attack that lures a victim by promising something desirable for free, such as a movie download or a USB drive left in a public place.

APEX technology group

Source: National Cybersecurity Alliance

SAMPLE PHISHING EMAIL

From: security-alerts@amaz0n-support.com
Subject: Urgent: Your Account Has Been Compromised!

Dear Customer,

We have detected suspicious activity on your Amazon account. Immediate action is required to prevent permanent suspension.

Please verify your account information by clicking the secure link below:

Verify Now

Failure to respond within 24 hours will result in account termination.

Thank you,
Amazon Security Team

WHAT'S WRONG?

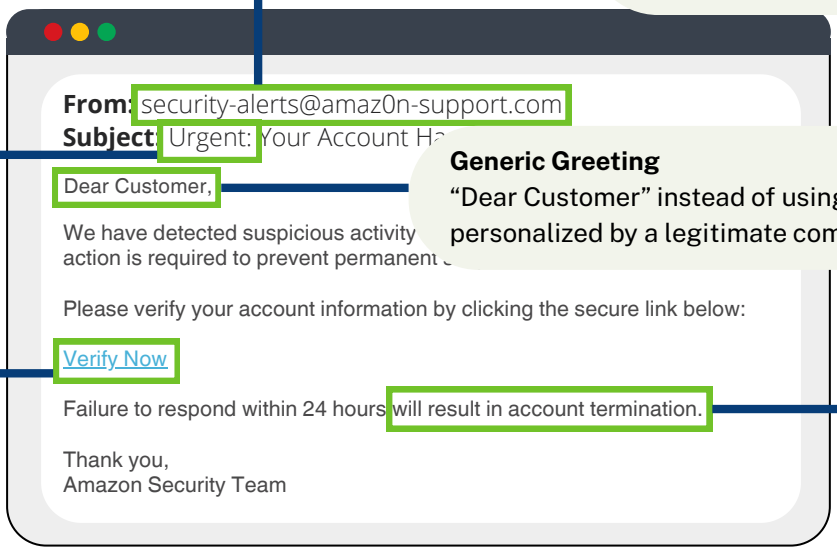
Suspicious Sender Address
"security-alerts@amaz0n-support.com" uses a misspelled domain ("amaz0n" instead of "amazon") and a non-official format.

Urgency & Threats
"Immediate action is required..." and "Failure to respond..." are classic urgency tactics to pressure you into acting without thinking.

Generic Greeting
"Dear Customer" instead of using your name is a sign it's not personalized by a legitimate company.

Fake Link
The link text says "Verify Now," but the actual URL is not Amazon. It's a deceptive domain: secure-login.com with "amaz0n-support" as a subdomain.

Unusual Consequences
Real companies don't threaten account termination over email without prior notice or multiple warnings.



APEX technology group