

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.

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.

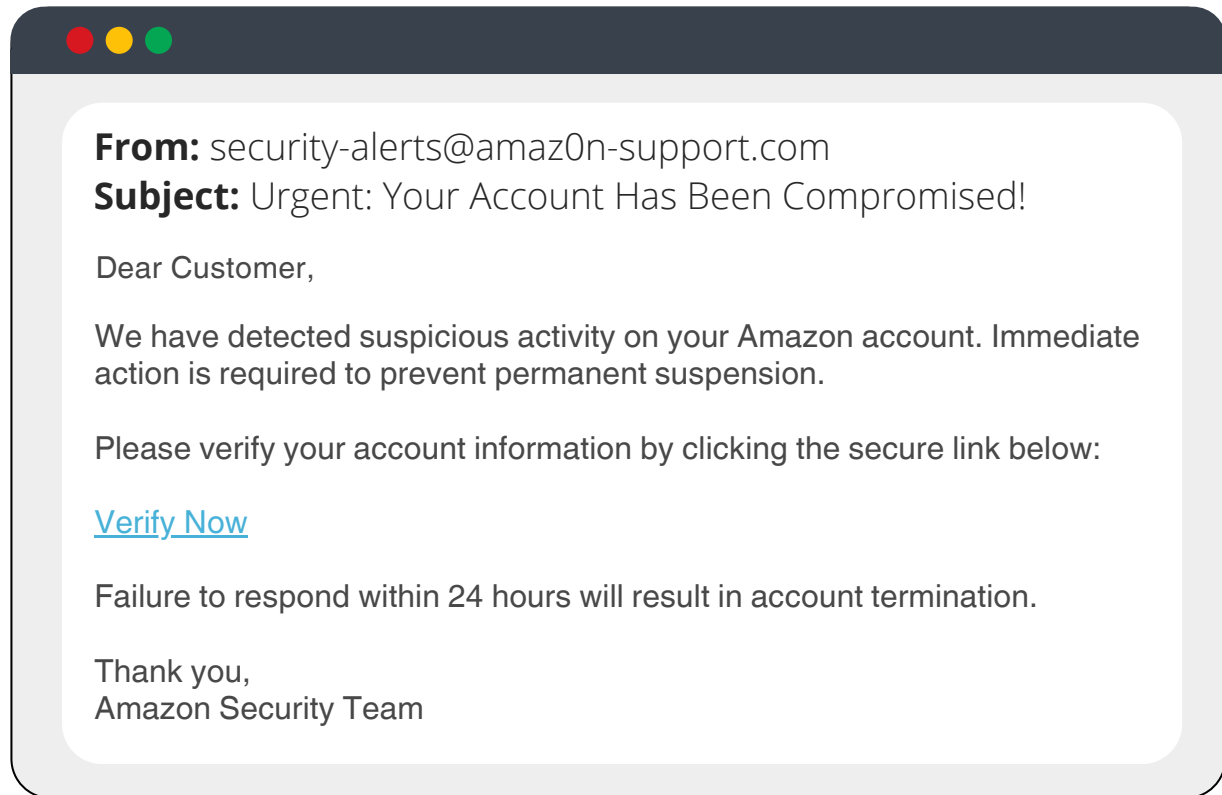
Pharming

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.

SAMPLE PHISHING EMAIL



WHAT'S WRONG?

Urgency & Threats

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

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.

Suspicious Sender Address

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

Generic Greeting

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

Unusual Consequences

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