SCAM SAFETY

A reference guide on how to recognize, avoid, and respond to email, web, and telephone scams

How to Use This Guide

Keep this guide somewhere accessible. If you encounter something you think could be a scam, you can reference the information on this document. Points written in black are relevant to all types of scams, while colored text indicates information about a specific type of scam.

What are Scams?

Scams aim to trick you into sending money, revealing personal information, or downloading malware onto your computer.

Scam Warning Signs

- Spelling or grammar errors are present.
- Incorrect, blurry, or outdated company logos are used.
- There is alarming or urgent messaging, such as a deadline.
- Correspondence uses a generic method of referring to you ("Hi dear," "Dear valued customer"), instead of your real name.
    - A legitimate company will use your name in its correspondence with you if it knows your name.
- Primarily email and web: urges you to click a link or download something. Companies typically do not ask you to download files via email. You should be able to find it through an official medium, such as their website.
- Email: The email address from a company uses a public domain instead of a company domain.
- Legitimate companies will use customized domains (customersupport@netflix.com) as opposed to free email providers (netflix@gmail.com).
- Email: It claims to be a company or colleague while the email address does not match or is a jumbled mess.
- Web: The site uses a URL unrelated to the company.
    - Watch out for subdomains; make sure the primary domain is legitimate.
- Telephone: The caller claims they are from a government organization that you have had no other contact with.
- Telephone: An automated sales call from a corporation or someone offering something for free.
- Telephone: The caller asks for personal information, or the voice is automated.

See scamsafety.kaveergera.com for more scam safety information.

Created as a part of Kaveer Gera's Eagle Scout Project.

Common Scam Tactics

- Offers a free gift card or prize.
- The message creates urgency or fear if you do not follow their instructions.
    - "Your account will be terminated in 24 hours! Click this link!" or "I'm stuck in another country, and I need money fast!"
- Impersonation: the scammer pretends to be a person or company you know.
    - Impersonates one of your friends or family asking for money for transport, for a project, to get out of jail, etc.
    - Claims a company sent you too much money and you must return the balance.
- The scammer uses similar characters in email addresses or URLs (rnark95@gmail.com instead of mark95@gmail.com) to fool you into thinking they're the right person.
- Primarily email and web: claims your computer has a virus which will delete all your files or reveal your personal information.
- Claims an account has been suspended and prompts you to click a link to reopen your account.
- Buttons often lead to elaborate spoof sites that imitate the legitimate site and steal the account information you enter.

Verifying Legitimacy

- Call the relevant company or person the potential scam is claiming to be.
    - Ensure you find their contact information independently of the information in the suspicious email, website, or phone call.
- Email: Check the email address the suspicious message was sent from.
    - If you do not recognize it as who the email sender is claiming to be, it is likely a scam.
- Email and web: Hover over links to see the linked URLs.
- Web: Check that the URL primary domain is the company the site claims to be.
- Telephone: Ask questions about the organization or ask them to reach out to you in another way.

What to Do If You Have Been Scammed

- Remain calm.
- If you shared or entered any passwords or personal information, immediately change the relevant passwords.
- If you sent any money, immediately contact your bank or other issuing financial institution to cancel the money transfer.
- If you downloaded a file, do not open it. Delete it and empty your trash/recycle bin, then run an antivirus scan.
- Don't be ashamed to seek help; scams happen to everyone.