How to Detect Fraudulent Emails

Scammers rely on a victim's curiosity to prompt a click or download of something dangerous. Think twice before downloading anything from the internet, especially if it's an attachment from an anonymous sender.

Publication date: July 19, 2021

What is Phishing?

Scammers will pretend to be someone you recognize in order to virtually "bait" you into sharing personal information. Scammers then use this information to gain access to your accounts. Phishing emails and texts may look like they're from a company you know or trust. Examples of phishing emails may include:

- An email posing as a Colorado state agency asking you to confirm your benefit account information.
- An email pretending to be from your healthcare insurance company asking you to confirm your Social Security number.
- An email that looks like it is from a well-known document sharing website asking you to collaborate on a document and enter your login credentials.
- An email trying to impersonate anti-virus software and prompting you to enter your credentials to avoid a virus.
- An email from a credit card company or bank asking you to take immediate action on an unpaid bill and enter your information.

What are the Harms of Phishing Schemes?

In each of the above situations the scammer will ask you to click on a link or enter personal information. The harms of falling for a phishing scheme include:

- **Compromising of your accounts**. If you enter your credit card number, login credentials, Social Security number or other information to a suspicious link, that information is no longer secure. If you use similar login credentials for several accounts, you should change login information for all of those accounts.
- **Identity theft.** Once a scammer has access to your personal information, they can impersonate you, obtain your credit, open accounts, and otherwise use your information in an unauthorized way.
- **Malware and ransomware.** If a hacker is able to trick you into entering your login credentials, they may be able to infect your system, lock your files, and demand payment for return of the files.

What should you do if the email is suspicious?

- **Confirm the sender's identity**. Hover over the sender's name to confirm the email address is correct. If you know the sender, but are still suspicious, reach out through a separate channel, like a phone call, to confirm that the sender actually sent the email.
- **Confirm the link is what it says it is.** Hover over any hyperlinks to confirm that they are directing you to a known, reliable website.
- **Look for typos or inaccuracies in the email.** Examine the email address, URL, and spelling used in any correspondence and that the context makes sense.
- **Set up two factor authentication, use strong passwords, and never use the same password across multiple accounts. There are many digital password managers available to help keep track of your passwords.**

Is the email suspicious?

High Risk:

an email that comes from an unknown sender with an attachment or link that you were NOT expecting.

Moderate Risk:

an email that comes from a known sender with an an attachment or link that you were NOT expecting.

Low Risk:

an email that comes from a known sender and has an attachment or link that you were expecting.

The Attorney General does not serve as legal counsel or advisor or provide legal advice, interpretation, or counsel to private citizens. Any information in this document constitutes only general statements and is not intended to serve as legal advice for any personal or specific situation.

If you notice any scams, fraud, price-fixing, unfair competition, or other attempts to take advantage of Coloradans, contact Stop Fraud Colorado at 800-222-4444 or www.StopFraudColorado.gov.