Let's Review!

- Watch out for:
  - Urgency and Fear
  - Vagueness
  - Evoking Sympathy
- What To Do:
  - Hang Up!
  - Delete the Text/Email
  - Block the Caller/Sender
  - Call a Trusted Number
  - Report the Scam
- Look for Other **Red Flags**:
  - Suspicious Links
  - Strange Email Address
  - Unconventional Payment Requests

Learn About Scams.org

Have questions, suggestions, or just want to reach out?

Visit our website at :
LearnAboutScams.org

Email us at:
contact@learnaboutscams.org

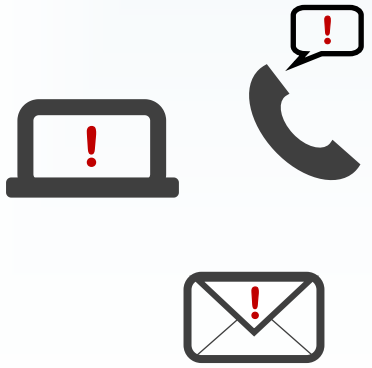
Disclaimer
LearnAboutScams.org will **NEVER** ask for your personal information or any form of payment.

Learn About Scams.org

How Do You Spot a

Scam?

Quick Tips for Identifying and Avoiding Common Scams



What does a scam look like?

Scams come in many forms, but here are a few things you can look out for:

- **Urgency and Fear**

  This is one of the most commons scam tactics: convince the victim they must act fast *or else*. If you're moving too quickly, you won't have time to stop and think about what you're doing, which is exactly what they want.

  Example: *If you don't pay now, we will send the police to your home.*

- **Vagueness**

  Scams will often make broad claims, usually reading from a script (or copying one) designed to fit a wide range of people. They're hoping that by using **urgency** you won't notice this.

  Example: *I'm calling from your insurance company…*

- **Evoking Sympathy**

  Scammers will try to make you feel bad for them, preying on your emotion in order to manipulate you.

  Example: *If you don't send this money I will lose my job.*

What should you do?

- **Hang Up The Phone!**

  If you're on the phone with an unknown caller and they exhibit one of these signs, hang up **immediately**.

- **Delete the Email/Text**

  If you notice a one of these tactics in an email or text message, do not respond (even if there is a STOP or "opt-out" option). Delete the message and do not reply to any further correspondence.

- **Block the Caller/Sender**

  If your phone or email provider gives you the option to block callers/ senders, do so as soon as possible. This will hopefully make it more difficult for the scammer to reach you in the future.

- **Call a Trusted Number**

  If you are not sure if it is a scam, hang up and dial a trusted number from that agency.

  Example: the bank's phone number on the back of your debit card.

- **Report the Scam**

  If you were scammed, call your local law enforcement. If you're comfortable using the internet, you can also visit **reportfraud.ftc.gov** or **complaint.ic3.gov** to report a scam.

Other Common Red Flags

- **Suspicious Links**

  It's best to avoid links sent via SMS/ Text. Only click on an email link if you are 100% certain of the source.

- **Strange Email Addresses**

  This one isn't always easy to spot. When in doubt, check the email address of the sender. Look out for addresses that don't correlate with the agency they claim to represent, emails claiming to be from large agencies with addresses *@gmail.com* or *@yahoo.com*, or slightly misspelled domains.*

  Here are a few examples:

  facebooksupport@gmail.com

  geeksquad@bestestbuy.com

  A "McAfee" email from: **adam.qtech@qtech.biz**

- **Unconventional Payment Requests**

  A legitimate company/agency will **NEVER** ask you to pay for something via gift cards or wire-transfer.

  If you are being asked to pay in gift cards, wire-transfer, or by mailing cash to someone, **IT IS A SCAM.**

*The domain is the part of the email address that comes after the "@" symbol, like "gmail.com".