

Key Points

Warning Signs

- You feel rushed, pressured, or intimidated.
- You are asked to provide personal, financial, or account information.
- You are asked to keep the conversation secret.
- An offer seems too good to be true (it probably is).
- They tell you to pay in a specific way, such as with gift cards or cryptocurrency.

If you suspect a scam...

- Ask someone you trust for a second opinion.
- Confirm requests using official contact information.
- Contact the FTC by calling their hotline at **877-382-4357**.

If something feels wrong, trust your instincts! It is *always* better to be safe than sorry.

Resources

Reporting scams can help prevent future scams. Report scams to the FTC at **ReportFraud.ftc.gov**

Worried your identity was stolen? Learn what to do at **IdentityTheft.gov**

National Elder Fraud Hotline
Call **(833) 372-8311**
Mon - Fri from 10 a.m. to 6 p.m.

For more information about scams and how to prevent them, visit **ScamEducation.org**

Being scammed is not your fault. Scams are a multi-billion dollar industry because scammers use dishonest and manipulative tactics. If you think you've been scammed, ***reach out for help.***

For attribution and licensing, visit ScamEducation.org/licensing

Identifying Email Scams



Identifying Scams



Check the Sender

Do you know this person?

Check the Email Address

Does the email address match the sender's name?



Check for Oddities

Does it look, sound, or feel strange? For example, it may have spelling mistakes.

Check the Subject Line

Is it urgent or threatening?



Check the Contents

Are they asking you to click a link or download a file?

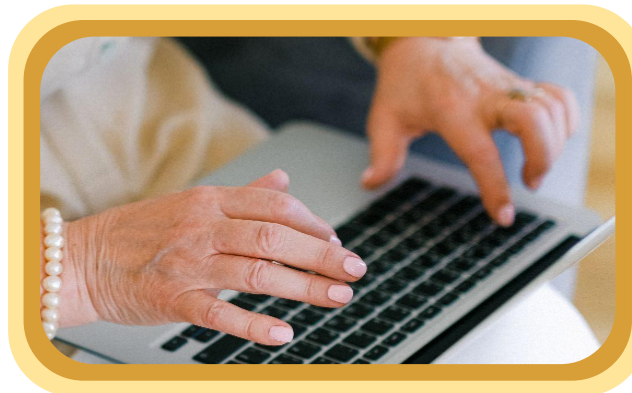
Check the Objective

Are they asking you to do something suspicious, like log into an account, send money, or share personal information?



Tips & Tricks

- Do not click links, buttons, or contact info in suspicious emails.
- Be very careful about sharing personal, financial, or account information by email.
- Never share a one-time code or password sent to you.



- Step away for a moment and think it over — especially if you feel rushed or pressured.
- If it seems too good to be true, it probably is.
- When in doubt, talk to a trusted person about your concerns.

Ending Scams



Step 1 - Block the Sender

This can stop them from emailing you again.

Step 2 - Report as Spam

Reporting the email can help stop future scams.



Step 3 - Delete the Email

This helps protect you from clicking harmful links or attachments by mistake.



You May Continue to Receive Emails

Scammers often use more than one email address and may try to contact you again. Stay alert and be cautious.