



What you don't
know can hurt you!

Let's walk through the agenda

- ▶ Quick refresher
- ▶ The latest scams happening today
- ▶ How to inspect emails and text messages to verify senders
- ▶ How to inspect web site links (e.g. buttons) before clicking on them
- ▶ How to utilize AI tools in spotting scams
- ▶ Checklist for any communication (email or text)
- ▶ How to use email and text junk blockers
- ▶ The benefit of freezing your credit and how to do so



Quick Refresher



Pause, reflect and protect!



Scammers play on your emotions and fears



2.6 million fraud reports and \$12.5 billion lost in 2024



Unsolicited phone calls that demand action



Text messages with links or phone numbers that elicit an emotional response



Phone calls from friends or family members that “sound” legit



What steps you can take if you suspect fraud

Latest Scams

- ▶ Customer support representatives sending you overdue bills with a phone number/website to get it resolved
- ▶ Emails from a person with an invoice PDF attachment that will install a computer virus to capture your keystrokes
- ▶ QR codes that direct you to a false website
- ▶ Robocalls using AI voices offering everything from vacations to auto warranties
- ▶ Refund scams targeting people who have been scammed in the past
- ▶ Deep fake technology showing celebrities supporting a medical miracle device or medication

Just when you think its real!



Who sent you that email or text?

- ▶ Let's first look at some emails and show you can know who sent you the email
 - ▶ Let's start with a valid email
 - ▶ Let's look at an obvious fake
 - ▶ Now a more subtle one
- ▶ Now I'll mirror my phone and we'll look at some text messages
- ▶ What did you learn?

It looks like a
valid “from”
email

- ▶ This means you have ruled out a SCAM. You've just confirmed that the email address seems valid.
- ▶ Scammers want some of the information to mostly true so you'll believe it.
- ▶ Keep checking!

Where is that link going?



- ▶ A link is some content (button, text, etc.) that when touched/clicked will bring you to some website
- ▶ Let's look at some examples of links first
- ▶ Next let's look at some actual emails and text message links
 - ▶ Let's do this with the web browser
 - ▶ Let's do this with an iPhone email
 - ▶ Let's do this with the Safari Browser on an iPhone
- ▶ What did you learn?

Turning on and off Link Preview

- ▶ Go to Settings
- ▶ Go to Apps (down the bottom)
- ▶ Go to Mail
- ▶ Find the Composing section
- ▶ Toggle the Add Link Previews option

Mark Addresses Off >

Increase Quote Level On >

Include Attachments
with Replies >

When Adding Recipients

Add Link Previews ☐

Signature >

Load Remote Images ☐

Default Account iCloud >

Messages created outside of Mail will
be sent from this account by default

What could indicate a scam?

- ▶ Address you personally or was it generic (like "Dear Customer")
 - ▶ Overly familiar (e.g. "wishing you well"), have misspelling or poor grammar
 - ▶ Unprofessional (poor formatting) or have the correct company logo
 - ▶ Sense of urgency to act right away to override your normal sense of caution
 - ▶ Company that you regularly do business with
 - ▶ Too good to be true
 - ▶ Attachments
-
- ▶ Let's look at some examples

How to use AI to spot scams

- ▶ Let's walk through an example of checking an email from Best Buy's Geek squad saying that your membership is up for renewal
- ▶ We'll use ChatGPT to verify the authenticity of the email
- ▶ Next let's use ChatGPT again to verify the authenticity of a text message
- ▶ I'll mirror my phone on the screen so you can follow along
- ▶ What did you learn?

Here's a quick checklist for any communication (email or text)

- ▶ Check the sender
- ▶ Check the links
- ▶ Address you personally or was it generic (like "Dear Customer")
- ▶ Overly familiar (e.g. "wishing you well"), have misspelling or poor grammar
- ▶ Unprofessional (poor formatting) or have the correct company logo
- ▶ Sense of urgency to act right away to override your normal sense of caution
- ▶ Company that you regularly do business with
- ▶ Too good to be true
- ▶ Attachments
- ▶ AI scanned
- ▶ Check with the source directly

Let's walk through the email and text junk identifiers

- ▶ We'll go through two popular email providers to tag an email as potential scam
 - ▶ Gmail
 - ▶ Yahoo
- ▶ Now let's use an iPhone to tag a text message as a potential scam
 - ▶ I'll mirror my phone so you can follow along
- ▶ What did you learn?