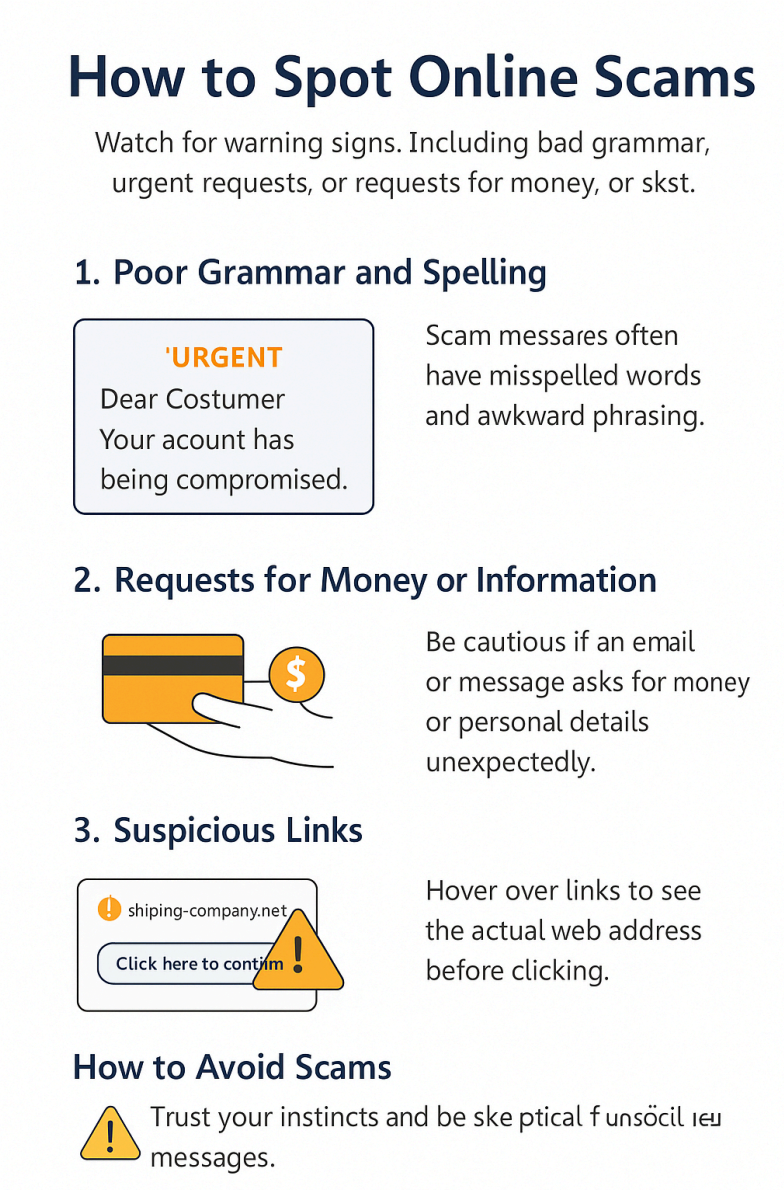



### What is phishing?

'Phishing' is when criminals use scam emails, text messages or phone calls to trick their victims. The aim is often to make you visit a website, which may download a virus onto your computer, or steal bank details or other personal information.

This page explains how to report phishing attempts,and protect yourself from scammers.

### How To Recognize Phishing

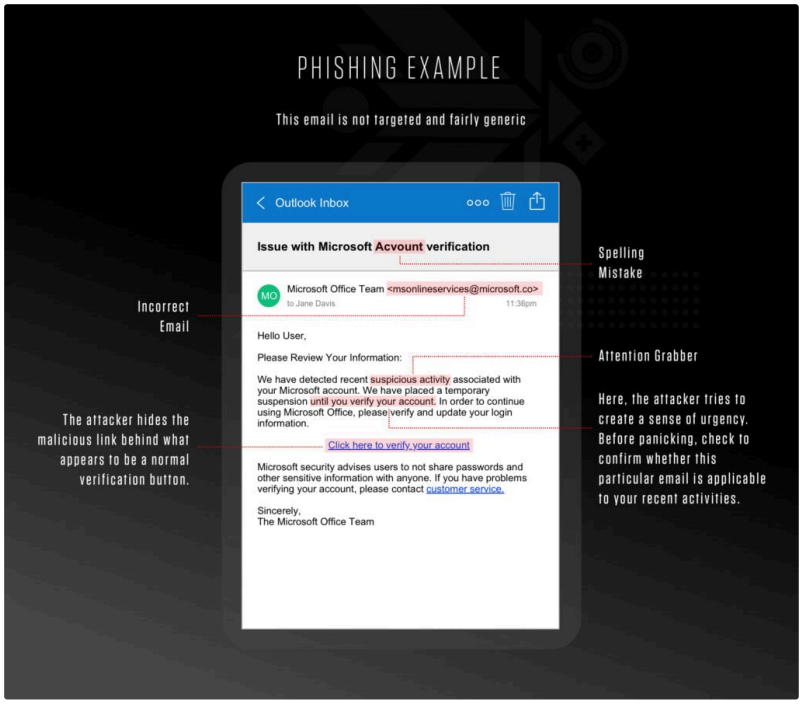
Scammers use email or text messages to try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could get access to your email, bank, or other accounts. Or they could sell your information to other scammers. Scammers launch thousands of phishing attacks like these every day — and they're often successful.

Scammers often update their tactics to keep up with the latest news or trends, but here are some common tactics used in phishing emails or text messages:

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. You might get an unexpected email or text message that looks like it's from a company you know or trust, like a bank or a credit card or utility company. Or maybe it's from an online payment website or app. The message could be from a scammer, who might

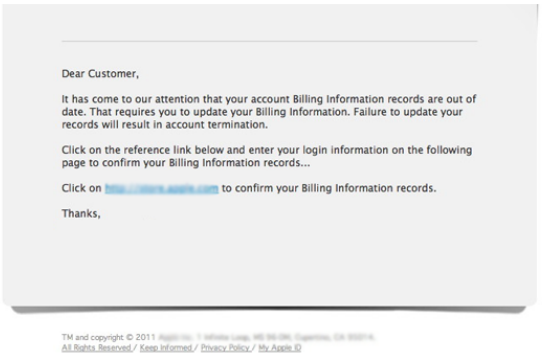
1. Asks for Sensitive Information
2. Uses a Different Domain
3. Contains Links that Don't Match the Domain
4. Includes Unsolicited Attachments
5. Is Not Personalized
6. Uses Poor Spelling and Grammar
7. Tries to Panic the Recipient

Here's a real-world example of a phishing email:

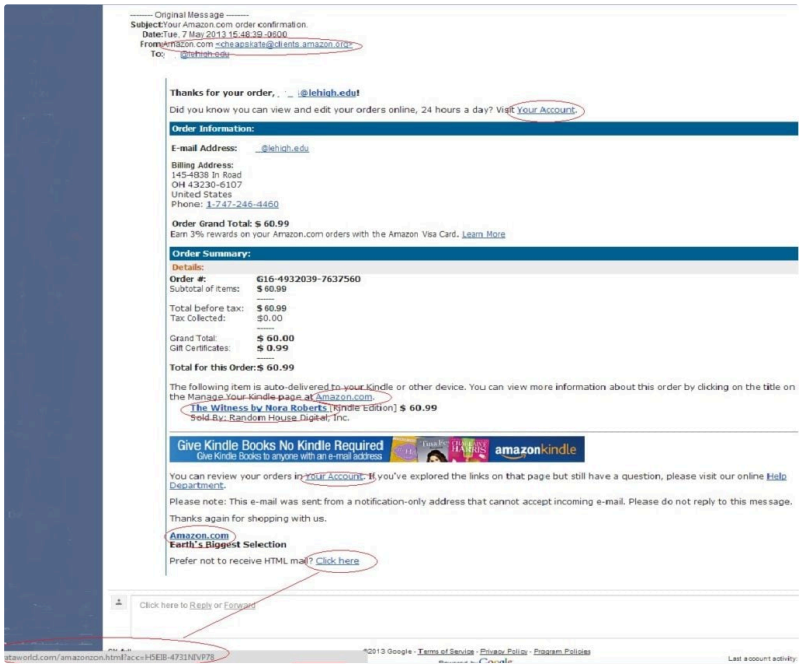

## 1. Asks for sensitive information

Legitimate businesses will never request credit card information, social security numbers or passwords by email. If they do, it's likely to be a scam



## 2. Uses a different domain

Phishing scams often attempt to impersonate legitimate companies. Make sure the email is sent from a verified domain by checking the 'sent' field. For example, a message from Amazon will come from @amazon.com. It won't come from @clients.amazon.org, like this phishing example:




## 3. Contains links that don't match the domain

In the above Amazon phishing example, you'll also see the links don't actually take you to the Amazon domain.

Hover the cursor over any links to make sure they will take you to the site you expect. Also, look for https:// at the start of the URL, and do not click links that do not use HTTPS.

## 4. Includes unsolicited attachments

A legitimate company will never attach or expect you to download files from their emails. It will instead direct you to its site, where you can download documents safely.

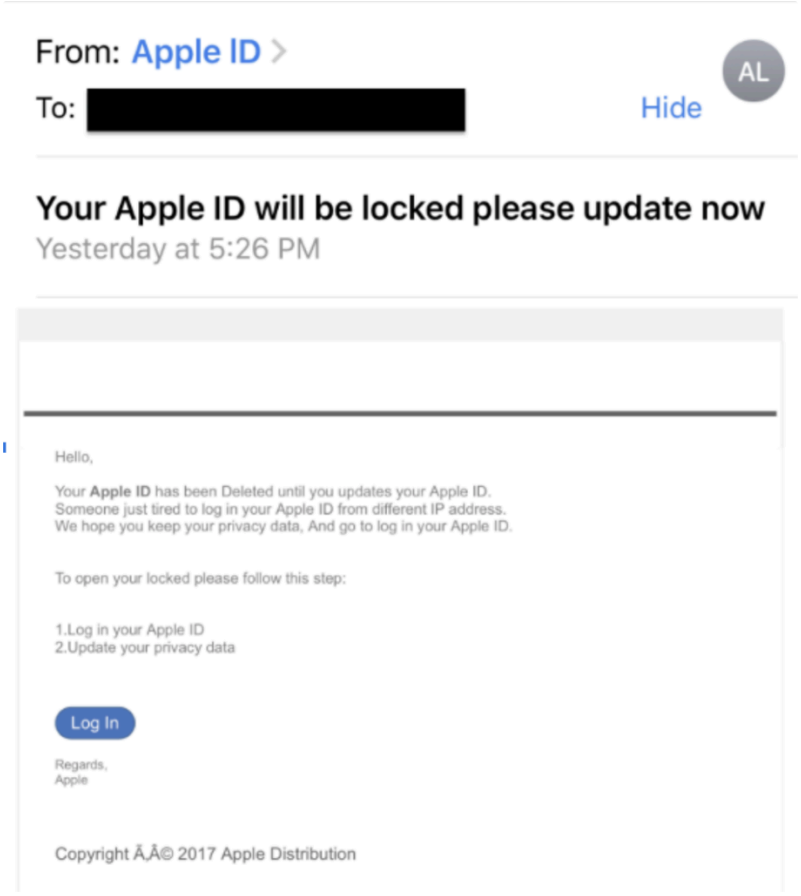
Avoid opening email attachments, even from a supposed well-known organization.

## 5. Is not personalized

Companies that do legitimate business – or whom you've shopped with previously – will know your name. And they will use it, rather than addressing you in a generic manner, such as "Dear Valued Member", "Dear Customer" or just "Hello".

## 6. Uses poor spelling and grammar

Official organizations employ specialist copywriters for their communications. They would never send out emails with obvious spelling or grammar errors, like this Apple phishing email example:




### Four Ways to Protect Yourself from Phishing

1. **Protect your computer by using security software**. Set the software to update automatically so it will deal with any new security threats.
2. **Protect your cell phone by setting software to update automatically.** These updates could give you critical protection against security threats.
3. **Protect your accounts by using multi-factor authentication.** Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication. The extra credentials you need to log in to your account fall into three categories:

- something you know — like a passcode, a PIN, or the answer to a security question.
- something you have — like a one-time verification passcode you get by text, email, or from an authenticator app; or a security key
- something you are — like a scan of your fingerprint, your retina, or your face

Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.

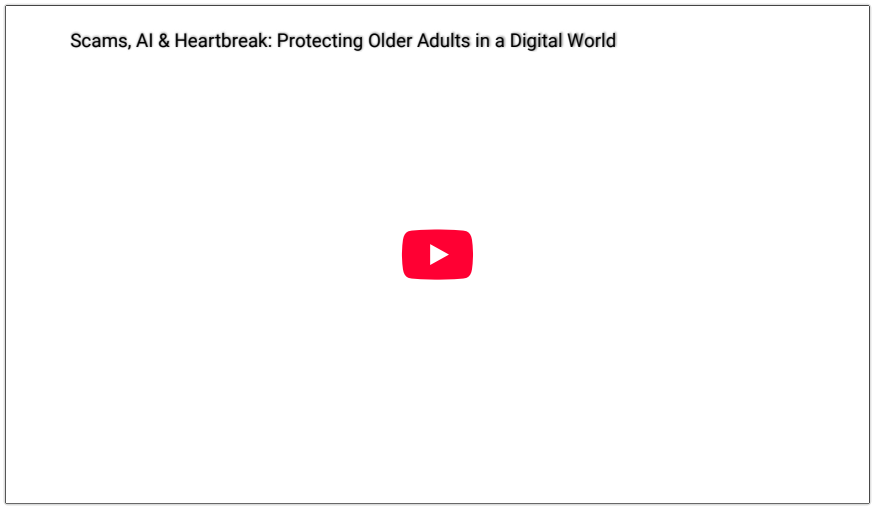
4. **Protect your data by backing it up.** Back up the data on your computer to an external hard drive or in the cloud. Back up the data on your phone, too.

## What To Do if You Responded to a Phishing Email

If you think a scammer has your information, like your Social Security, credit card, or bank account number, go to IdentityTheft.gov. There you'll see the specific steps to take based on the information that you lost.

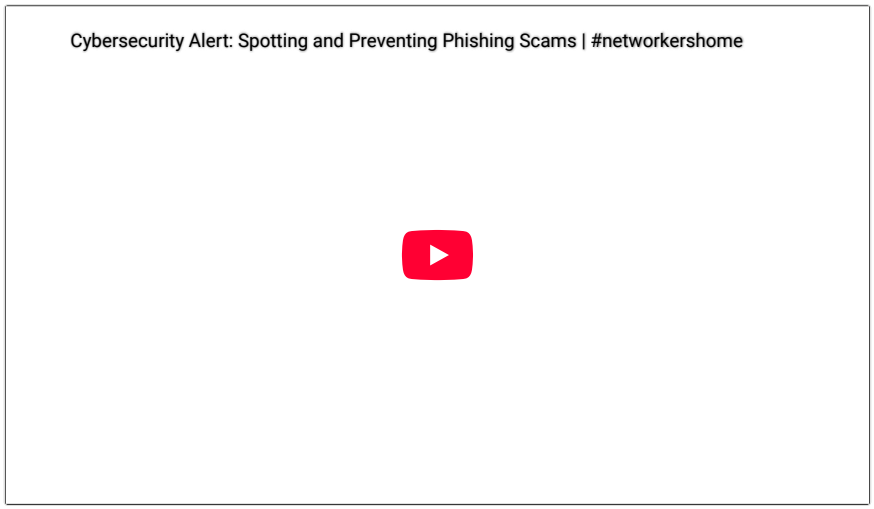
If you think you clicked on a link or opened an attachment that downloaded harmful software, update your computer's security software. Then run a scan and remove anything it identifies as a problem.

Scams, AI & Heartbreak: Protecting Older Adults in a Digital World



A recent (2 weeks ago) video aimed at older audiences, covering scam warning signs like suspicious prompts, call verification, and social media security.

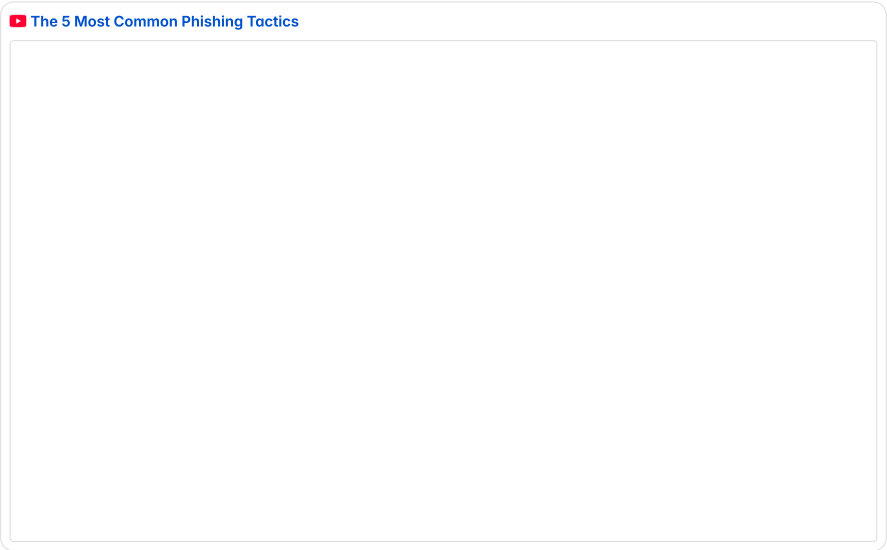
Cybersecurity Alert: Spotting and Preventing Phishing Scams | #networkershome



A practical guide detailing phishing techniques and how to safeguard yourself against email and web-based scam attempts.

How To Protect Seniors From Phone Scams? - CountyOffice.org

A recent, practical walkthrough showing real phone scam scenarios and step-by-step tips to spot and avoid them.



| Scams Covered | Key Visual Cues & Prevention Tips |
| --- | --- |
| **Phone Scams** | Listen for urgent, pushy language (“You’re in trouble!”). Verify caller info by hanging up and redialing from official sources. |
| **Online/Dark Web Scams** | Notice suspicious URLs, spelling mistakes or masked links — avoid clicking. Use secure (HTTPS) sites only. |
| **Tech Support Scams** | Scammers often ask you to open Task Manager or click “Yes”. Never allow remote access. Hang up and contact the official provider. |