


# **4 EASY WAYS** to stay safe **online**

Our online world needs to be protected. There are easy things we can do to ensure our information is safe from those wishing to steal it.



## **Recognize & report phishing**



Most successful online intrusions result from a recipient of a “phishing” message accidentally downloading malware or giving their personal information to a spammer. Do not click or engage with these phishing attempts. Instead, recognize them by their use of alarming language or offers that are too good to be true.

**Report the phish and delete phishing messages.**

## **Use strong passwords**

Simple passwords can be guessed. **Make passwords at least 16 characters long**, random and unique for each account. Use a password manager, a secure program that maintains and creates passwords. This easy-to-use program will store passwords and fill them in automatically on the web.

\*\*\*\*\*



## **Turn on multifactor authentication (MFA)**

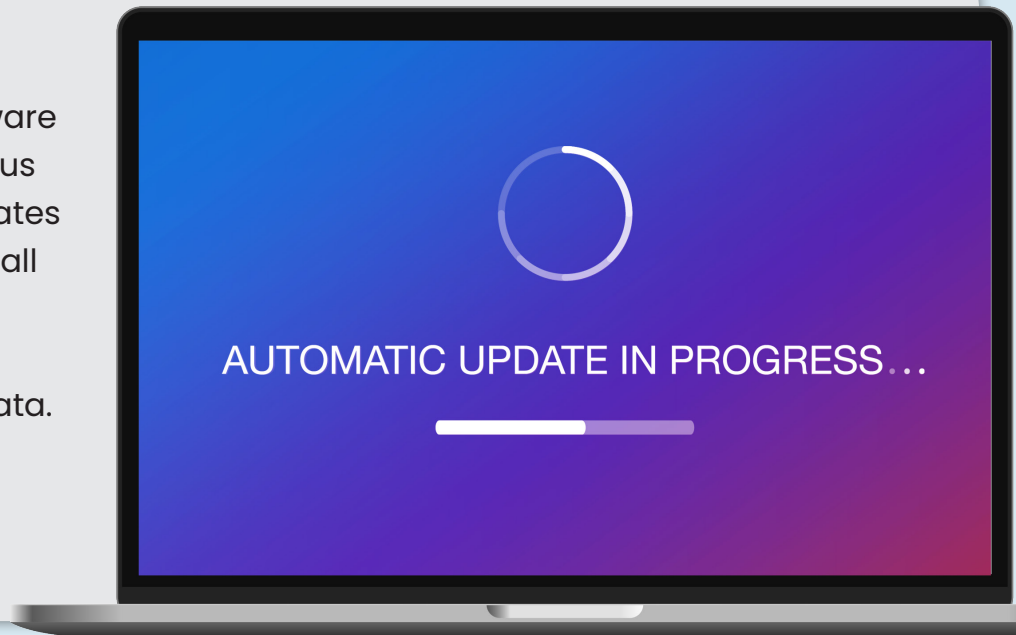
Use MFA on any site that offers it. MFA provides an extra layer of security in addition to a password when logging into accounts and apps, like a face scan or a code sent by text.

**Using MFA will make you much less likely to get hacked.**

## Update software

When devices, apps or software programs (especially antivirus software) notify us that updates are available, we should install them as soon as possible. Updates close security code bugs to better protect our data.

**Turn on automatic updates to make it even easier.**



Taking these steps helps  
**Secure Our World.**



**We can all help one another**  
stay safer online, so share these tips  
with a family member or friend!

[cisa.gov/SecureOurWorld](https://cisa.gov/SecureOurWorld)

# OUTSMART

## online outlaws

### Avoid Phishing Scams with Three Simple Tips

Phishing scams are online messages designed to look like they're from a trusted source. We may open what we thought was a safe email, attachment or image only to find ourselves exposed to malware or a scammer looking for our personal data. The good news is we can take precautions to protect our important data. Learn to recognize the signs and report phishing to protect devices and data.



# 1

#### Recognize the common signs

- Urgent or emotionally appealing language
- Requests to send personal or financial information
- Unexpected attachments
- Untrusted shortened URLs
- Email addresses that do not match the supposed sender
- Poor writing/misspellings (less common)



# 2

#### Resist and report

**PHISHING****SPAM**

Report suspicious messages by using the "report spam" feature. If the message is designed to resemble an organization you trust, report the message by alerting the organization using their contact information found on their webpage.

# 3

#### Delete

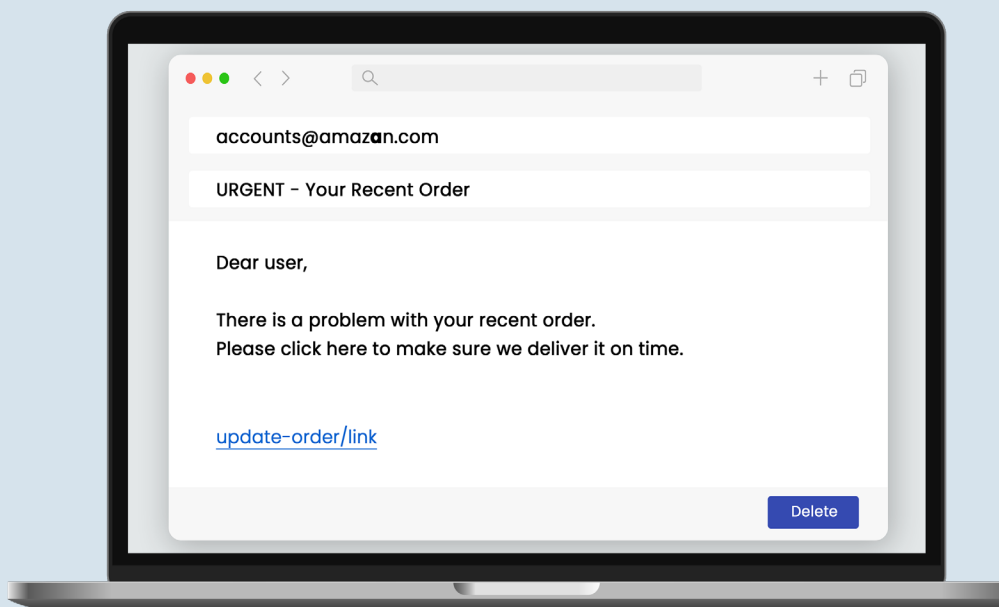
Delete the message. Don't reply or click on any attachment or link, including any "unsubscribe" link. The unsubscribe button could also carry a link used for phishing. **Just delete.**

**DELETE**

# If a message looks suspicious, it's probably phishing.

But even if there's a possibility it could be real, don't click any link, attachment or call any number. Look up another way to contact a company or person directly:

- Go to a company's website to find their contact information
- Call the individual at a known number and confirm whether they sent the message



## Avoiding phishing is one way to **Secure Our World.**



**We can all help one another**  
stay safer online, so share these tips  
with a family member or friend!

[cisa.gov/SecureOurWorld](https://cisa.gov/SecureOurWorld)