SECURE OUR WORLD

CISA
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

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)

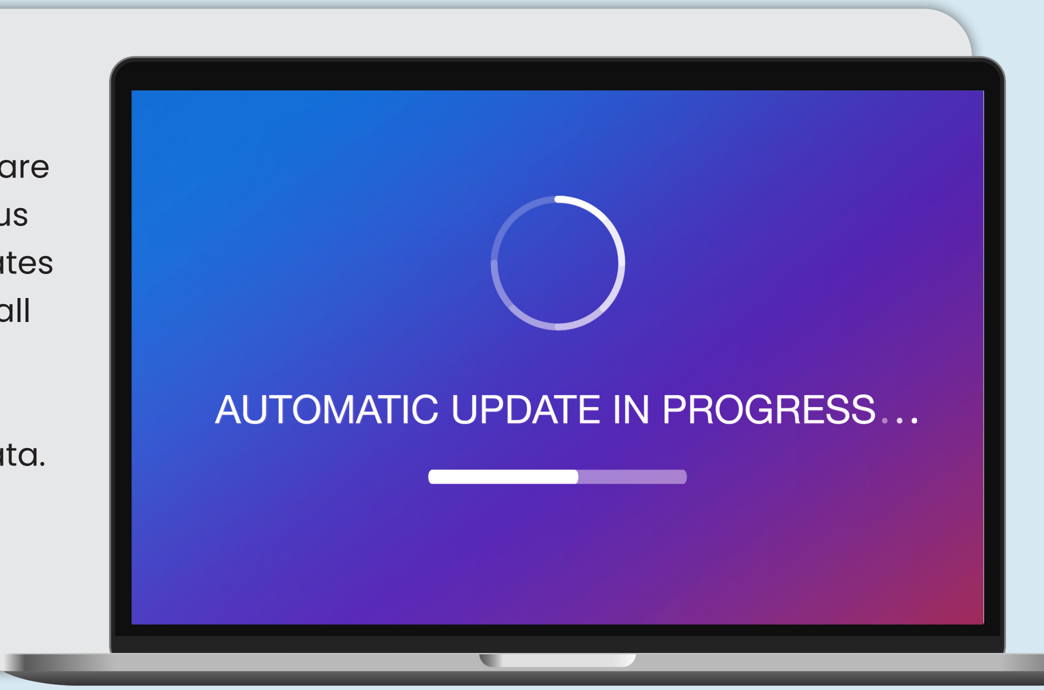
Use MFA on any site that offers it. MFA provides an extra layer of security in addition to a password when logging into accounts and apps, like a face scan or a code sent by text.

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

cisa.gov central@cisa.dhs.gov @CISA.gov | @CISACyber @cisa.gov As of August 14, 2023

SECURE OUR WORLD

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

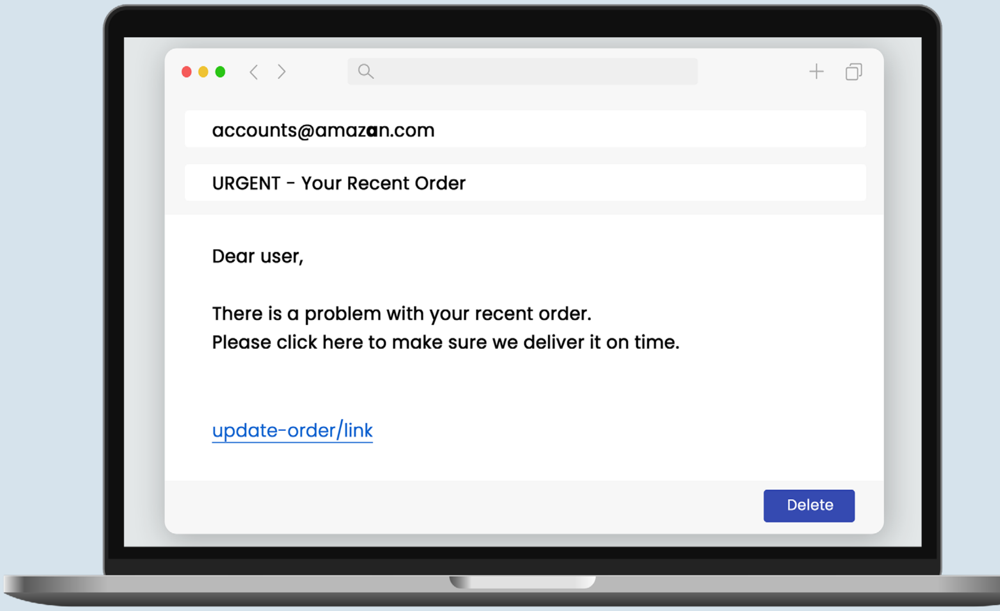
Delete the message. Don't reply or click on any attachment or link, including any "unsubscribe" link. The unsubscribe button could also carry a link used for phishing. **Just delete.**

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



accounts@amazan.com

URGENT - Your Recent Order

Dear user,

There is a problem with your recent order.
Please click here to make sure we deliver it on time.

update-order/link

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

SECURE OUR WORLD

Weak PASSWORDS are the most common way **online criminals** access accounts

Strengthen Passwords with Three Simple Tips

Using strong passwords with the help of a password manager is one of the easiest ways to protect our accounts and keep our information safe.

1 Make them long

At least 16 characters—longer is stronger!

****

2 Make them random

Two ways to do this are:

Use a random string of letters (capitals and lower case), numbers and symbols (the strongest!):

cXmnZK65rf*&DaaD

Create a memorable passphrase of 5-7 unrelated words:

HorsPerpleHatRunBayconShoos

Get creative with spelling to make it even stronger.

3 Make them unique

Use a different password for each account:

k8dfh8c@Pfv0gB2

LmvF%swVR56s2mW

e246gs%mFs#3tv6

Tip! Use a password manager to remember them.

Let a password manager do the work!

A password manager creates, stores and fills passwords for us automatically. **Then we each only have to remember one strong password**—for the password manager itself. Search trusted sources for "password managers" like Consumer Reports, which offers a selection of highly rated password managers. Read reviews to compare options and find a reputable program for you.

When we choose strong passwords, we make it much harder for someone to steal our:

Data **Money** **Identities**

Using strong passwords 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

SECURE OUR WORLD

Stay **safer** with

MULTIFACTOR AUTHENTICATION (MFA)

How to turn on MFA

MFA provides extra security for our online accounts and apps. This security could be a code sent via text or email or generated by an app, or biometrics like fingerprints and facial recognition. Using MFA confirms our identities when logging into our accounts.

Follow these easy steps on each account

Go to Settings

It may be called Account Settings, Settings & Privacy or similar.

Look for and turn on MFA

It may be called two-factor authentication, two-step verification or similar.

Multifactor Authentication ●

Confirm

Select how to provide extra login security, such as by entering a code sent via text or email or using facial recognition.

Congratulations!

After setting up MFA, logging in may require completing the MFA security step to prove our identities. It only takes a moment but makes us **significantly safer from malicious hackers!**

Turn on MFA for every online account or app that offers it. Doing so will protect our:

- **Email**
- **Banking**
- **Social Media**
- **Online Purchases**
- **Identities**

Using MFA 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

Install SOFTWARE UPDATES to fix security risks

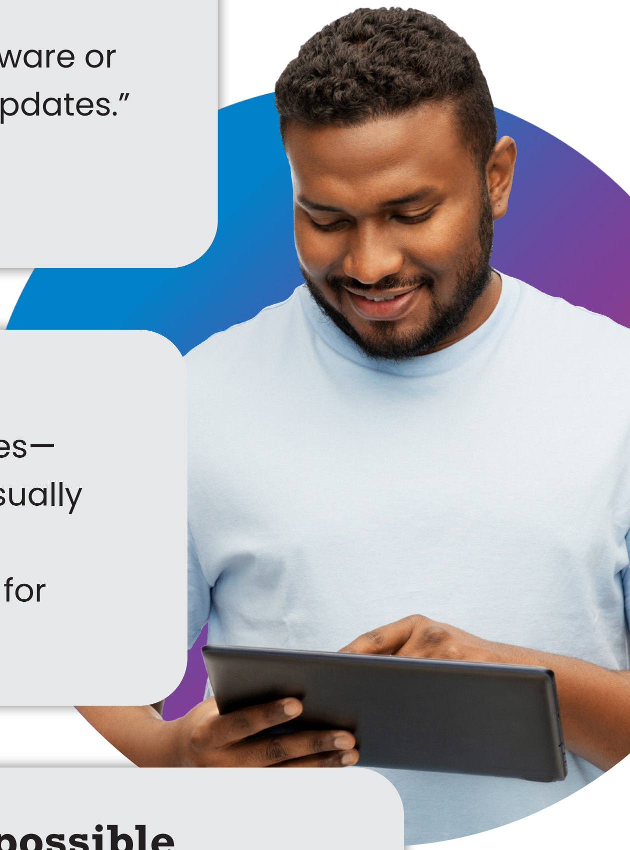
Update Software Promptly for Safety

When we see an update alert, many of us tend to hit “Remind me later.” Think twice before delaying a software update! Keeping software up to date is an easy way to stay safer online. **To make it even more convenient, turn on automatic updates!**

Turn on automatic updates

Look in the device’s settings, possibly under Software or Security. Or search the settings for “automatic updates.”

Automatic Updates ●



Watch for notifications

Not every update can be automatic. Devices—mobile phones, tablets and laptops—will usually notify us that we need to run updates. It’s important to install ALL updates, especially for **web browsers and antivirus software.**

Install updates as soon as possible

When notified about software updates, especially critical updates, install them as soon as possible. Online criminals won’t wait so we shouldn’t either!

Why it’s so important to update promptly

If a criminal gets into a device through a security flaw, they will look for personal information and sensitive data to exploit. Technology providers issue software updates to “patch” security weak spots as quickly as possible.
If we don’t install them, they can’t protect us!

Software updates can also:

Fix Bugs

Improve Performance

Install Latest Features

Updating software 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