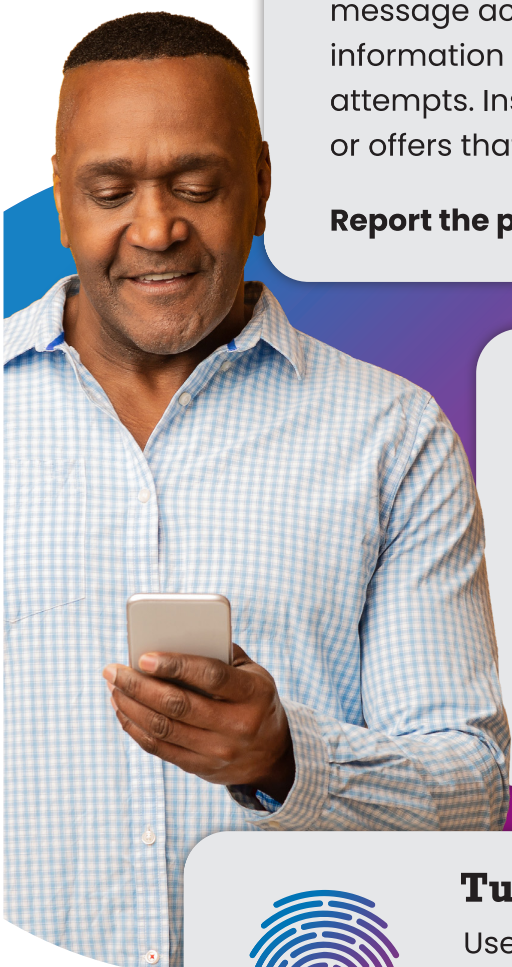
4 EASY WAYS
to stay safe **online**

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.

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

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.

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.

Install SOFTWARE UPDATES to fix security risks

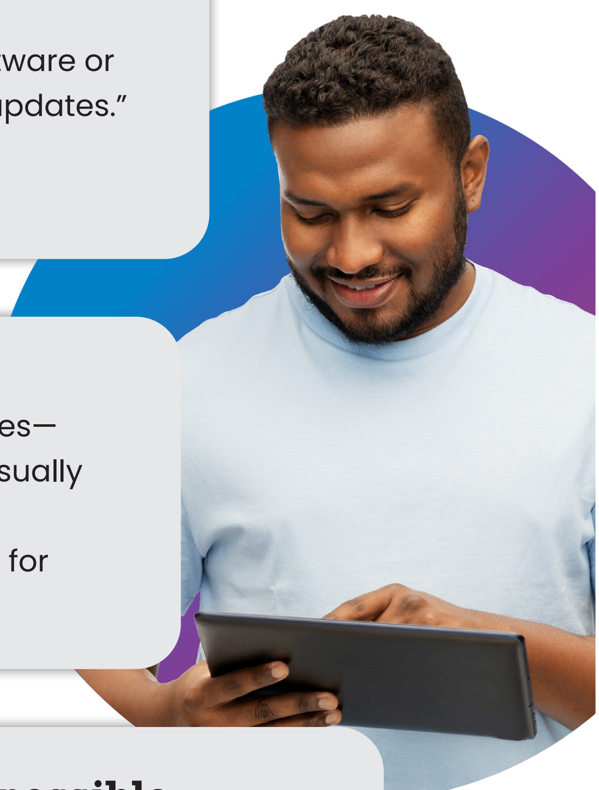
Update Software Promptly for Safety

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

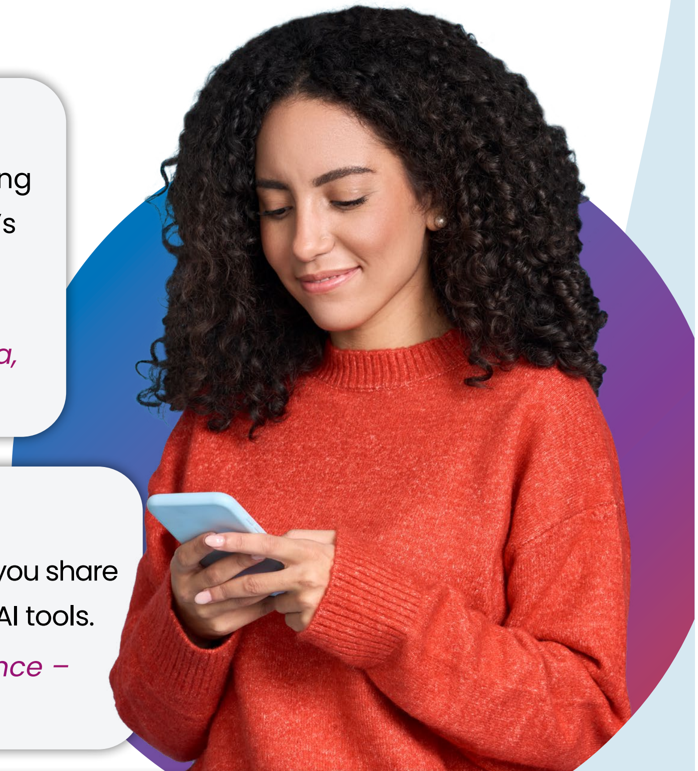
Not every update can be automatic. Devices—mobile phones, tablets and laptops—will usually notify us that we need to run updates. It's important to install ALL updates, especially for **web browsers and antivirus software.**

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!

STAY SAFE ONLINE WHEN USING AI

While AI might offer valuable capabilities, always remember to stay proactive and educated about the risks. Here are essential tips to ensure you stay secure while using generative AI.



1. Mind Your Inputs

AI systems learn from user inputs, so refrain from sharing anything you want to keep private, like your workplace's company data or your personal details.

TIP: *Avoid sharing sensitive or confidential information with AI models – if you wouldn't post it on social media, don't share it with AI.*

2. Be Privacy Aware

Since AI models often scrape data from the web, what you share publicly online may be copied, in whole or in part, by AI tools.

TIP: *Think about what you share with a wide audience – would you want an AI to have it?*

3. How Hackers Use AI

Cybercriminals may use AI to fool you. Public tools can mimic a person's voice or image (this is sometimes called a "deepfake"). Criminals can make a voice call to mimic a trusted person and steal money or to harass people by posting fake or modified images and videos.

TIP: *Stay updated on cybersecurity best practices. Criminals using AI as a tool makes it more important that everyone protect themselves using the core 4 behaviors: strong passwords, MFA, software updates, and reporting phishing.*

4. AI is a Tool

While AI can assist with tasks, it's important to maintain your expertise and not rely solely on AI-generated content. Prompting isn't the same as creating!

TIP: *Treat AI as a helpful tool rather than a replacement for your skills.*

RAISING DIGITAL CITIZENS

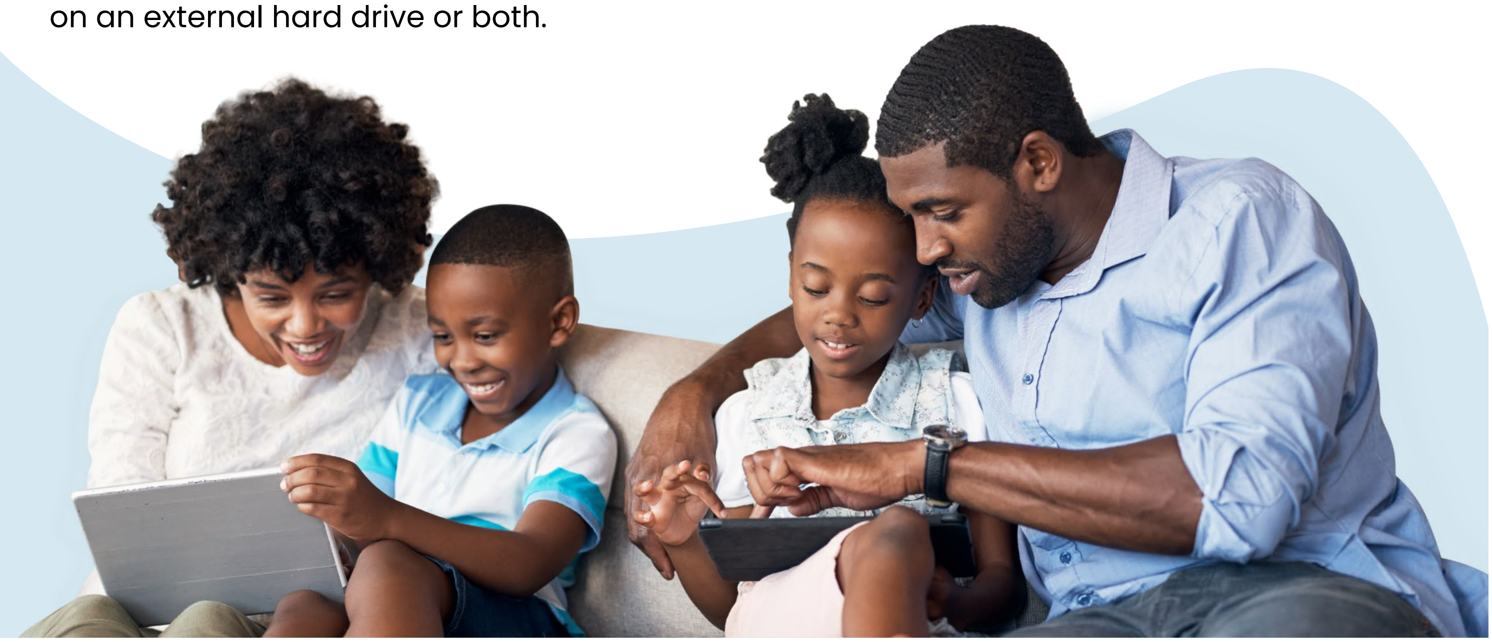
We all know the internet is a fantastic world of learning and entertainment for kids, but, like the real world, there can be dangers, too. With some precautions, you can set your children up to become upstanding digital citizens that will lead the future. On the other hand, giving children uninhibited access to the internet can put your child, computer and personal data at risk.

Remain positively engaged

Pay attention to the online environments your children use. Surf the web with them. Appreciate your children's participation in their online communities and show interest in their friends. When they encounter inappropriate material, react constructively and make it a teachable moment.

Keep a clean machine

Cybersecurity starts with protecting all household computers with a security suite, meaning antivirus, antispyware and firewall software. Software companies often send updates that deal with the latest cybersecurity threats, so set your software to update automatically so you don't have to worry about it. Keep your operating system, web browsers and other software current as well. Importantly, back up computer files regularly either on the cloud, on an external hard drive or both.



Double Puzzle

Solve the anagrams and use the circled letters in the top part to complete the final phrase at the bottom. Each circled letter is used just once.

AOSDRPWS

TNRETENI

UTDPEA

YRISTCEU

PYRICAV

PECTOMUR

AEKCHR

EEICVD

IWIF

RCEBY

IRYFEV

ELARMWA

GOILN

Double Puzzle Answer Key

AOSDRPWS	P A S S W O R D
TNRETENI	I N T E R N E T
UTDPEA	U P D A T E
YRISTCEU	S E C U R I T Y
PYRICAV	P R I V A C Y
PECTOMUR	C O M P U T E R
AEKCHR	H A C K E R
EEICVD	D E V I C E
IWIF	W I F I
RCEBY	C Y B E R
IRYFEV	V E R I F Y
ELARMWA	M A L W A R E
GOILN	L O G I N

S T A Y   S A F E   A N D   S E C U R E
O N L I N E