THE INTERNET SURVIVAL GUIDE

for adults 60+



What you'll find in this guide:

- Know Your Surroundings
- Your Survival Kit
- Your Biggest Threats
- Emergency Response

Powered by PHIN

KNOW YOUR SURROUNDINGS

What do these mean?

Cybersecurity comes with a lot of jargon. Here's what you actually need to know.

- **Phishing:** A fake email designed to trick you into clicking a link, sharing information, or sending money.
- **Smishing:** Phishing by text message.
- **Vishing:** Phishing by phone call or voicemail.
- **Qishing:** A fake or malicious QR code that sends you to a dangerous website.
- **Deepfake:** AI-generated video or audio designed to make it look or sound like a real person said or did something.
- **MFA** (multi-factor authentication): An extra security check at login, like a code sent to your phone.



RED FLAGS TO LOOK OUT FOR

🚩 **Urgency:** You're told to act, pay, click, or respond immediately.

🚩 **Money:** Someone unexpectedly asks for money, gift cards, cryptocurrency, or banking information.

🚩 **Passwords and codes:** You're asked to share a password, login code, or other security information.

🚩 **Secrecy:** Someone tells you not to speak to your bank, friends, or family.

🚩 **Something looks off:** The email address, phone number, spelling, or website address doesn't look quite right.

🚩 **Too good to be true:** You've won something you didn't enter, or you're promised easy or guaranteed money.



See a red flag? Slow down before you click, reply, pay, or share anything.

YOUR SURVIVAL KIT

For help setting anything up, reach out to your IT provider or someone you trust.

Slow down. Scammers love urgency. If someone says you need to pay, click, transfer money, or share information right now, that's a reason to stop.

Use different passwords for every account. If someone gets access to your password, you don't want them to gain access to *all* your accounts.

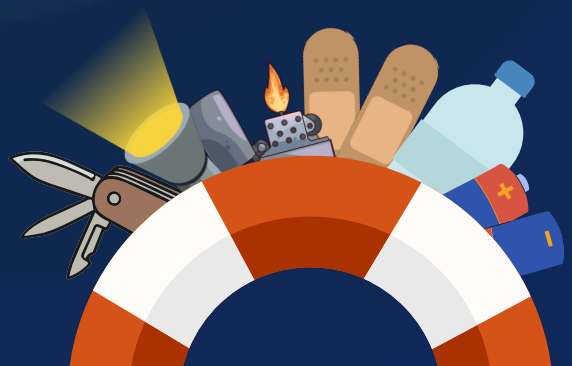
Enable automatic system updates on your devices. Most updates fix security issues.

Keep your passwords in a safe place. A password manager securely stores your passwords, so you don't have to remember them all.
If you prefer writing passwords down, keep the notebook somewhere private and secure, not next to your computer.

Lock your devices. Use a PIN, password, fingerprint, or face recognition, and lock devices whenever you step away from them.

Set up MFA. If you get a verification code when you're not actively logging into an account, you know someone else is trying to access your account and you can report it. And never give that code to someone else.

Enable fraud alerts with your bank and credit cards so you're aware of unusual payments.



ALWAYS PAUSE & PONDER:

Who sent this?

Do you recognize the **actual** email address or phone number, not just the name displayed?

What are they asking for?

Do they want money, banking information, passwords, login codes, or personal information? Legitimate organizations should not unexpectedly ask you to hand over passwords or security codes.

Why are they reaching out & does it make sense?

Ask yourself:

- Do I know this person?
- Do I even have an account with this company or bank?
- Is my relative really in trouble?
- Did I actually enter that competition?
- Was I expecting this message or call?

When do I need to respond?

Urgency is a major red flag. Be suspicious of phrases like “RIGHT NOW,” “FINAL WARNING,” “ACT IMMEDIATELY,” or “YOUR ACCOUNT WILL BE CLOSED.” A genuine request can usually survive a few minutes while you check it.

Where can I verify their request?

Never be embarrassed to check. Open the organization’s official app, type its website address yourself, or contact the person or company using details you already trust. **Don’t use the phone number, link, or contact details in the suspicious message itself.**

YOUR BIGGEST THREATS

1 "THERE'S A PROBLEM WITH YOUR ACCOUNT"

Someone claiming to represent your bank, Amazon, a government agency, or another familiar organization says something has gone wrong. They need your password, verification code, card details, or money to fix it.

What should you do? Stop the conversation and contact the organization independently using its official website, app, or a number you already trust.

2 "MOM/DAD/GRANDMA/GRANDPA, I NEED HELP"

Someone has a new phone number. They've lost their wallet, they're stranded somewhere, or they need money urgently. Scammers can use information from social media to make the story convincing, and can even use AI to imitate somebody's voice or image.

What should you do? Hang up and contact your relative using the number you already have. Consider agreeing on a family "safe word" that can be used to verify someone's identity in an emergency.

3 "YOUR COMPUTER HAS A VIRUS"

A caller or pop-up claims your computer has been infected and offers to fix it. They may ask you to install software that gives them remote access to your device.

What should you do? Don't install anything or give anyone remote access because of an unexpected call or pop-up. Close it and contact someone you trust if you're concerned.





"YOU'VE WON!"

Congratulations! Unfortunately, the prize requires an upfront payment, gift card, cryptocurrency transfer, or your banking information before you can receive it.

What should you do? Keep your money. Genuine prizes don't require you to pay to collect your winnings.



"WE HAVE A REAL CONNECTION"

Romance and friendship scams can develop over weeks or months. Someone builds a genuine-feeling relationship before an emergency, investment opportunity, travel problem, or other reason for needing money suddenly appears.

What should you do? Never send money or financial information to someone you only know online. Talk to somebody you trust if an online relationship starts involving money.



"YOUR WARRANTY IS ABOUT TO EXPIRE"

If you receive a warranty for your car in the mail but you've never bought a warranty before, don't respond. "If you receive an unexpected medical bill, especially for an appointment you never had, don't respond.

What should you do? Any unexpected or urgent payment requests received by mail should be verified using a phone number you trust—not the number provided in the bill or letter.

WHEN IN DOUBT, LOOK UP THEIR PHONE NUMBER AND CALL THEM BACK.

OH, CRAP.
I FELL FOR A SCAM.

Now what?

Scams work because criminals are very good at creating panic, trust, excitement, or embarrassment. Speaking up quickly could help you recover an account or payment, and you could stop someone else from falling for the same trick.

STEP 1

Stop communicating with the scammer and don't send any more money, passwords, information, or verification codes, even if they claim doing so will fix the problem.

STEP 2



If you shared banking or card information, contact your bank or card provider immediately.



If you gave away a password, change it anywhere you've used it and enable MFA.



If someone gained access to your computer, disconnect it from the internet and get help from someone you trust.

STEP 3

Don't be embarrassed. **Tell someone you trust** and report the scam.

In the US, you can report fraud to the Federal Trade Commission at ReportFraud.ftc.gov and internet crime to the FBI's Internet Crime Complaint Center (IC3) at ic3.gov.