THE INTERNET SURVIVAL GUIDE

for young adults



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?

You've probably spent most of your life online. Unfortunately, so have scammers. Here are a few terms worth knowing.

Phishing: A fake email that tricks you into clicking, sharing info, or sending money.

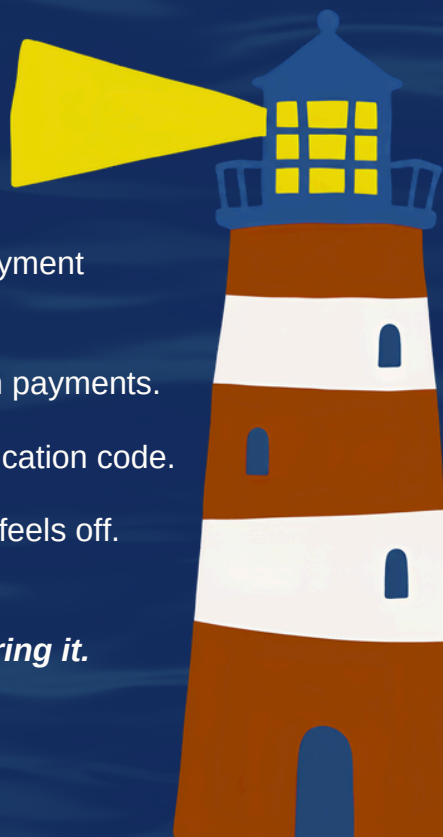
Smishing: Phishing by text message.

MFA (multi-factor authentication): An extra check at log-in, like a code sent to your phone.

Deepfake: AI-made video, images, or audio that imitates a real person.

Malware: Harmful software that steals info, spies on you, or damages your device.

Major red flags to look out for:



🚩 **Urgency:** You need to pay, reply, click, or act right now.

🚩 **Easy money:** Huge returns, suspiciously well-paid jobs, or free stuff for little work.

🚩 **Moving off-platform:** Someone quickly wants to take the chat or payment elsewhere.

🚩 **Unusual payments:** Gift cards, crypto, wire transfers, or off-platform payments.

🚩 **Passwords and codes:** Someone asks for your password or a verification code.

🚩 **Something doesn't add up:** The URL, email, profile, price, or story feels off.

Trusting your gut isn't a cybersecurity strategy, but neither is ignoring it. Stop and check.

YOUR SURVIVAL KIT

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

Use different passwords. Reusing one means a single compromised account can unlock *all* the others.

Use a password manager. It creates and stores strong passwords. Better than guessing whether you ended with 1, !, or 1!.

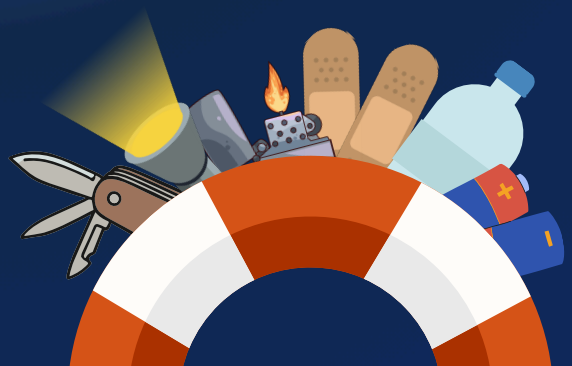
Check your privacy settings. Know who can see your posts, location, contact details, and other personal information. Be especially careful about publicly sharing your address, workplace, regular locations, travel plans, or anything commonly used in security questions.

Know how to verify things. Don't use contact details from a suspicious message. Open the official app or type the website yourself.

Set up MFA, especially for email, banking, social media, shopping, and anywhere that stores payment info.

Turn on automatic updates for your phone, computer, browser, and apps. Updates often fix security weaknesses as well as adding whatever feature nobody asked for.

Lock your devices. Use a PIN, password, fingerprint, or face recognition and set devices to lock automatically.
Your phone probably contains your email, banking, photos, messages, passwords, and half your life. Protect it accordingly.



Before you click, pay, download, share, or reply:

ALWAYS PAUSE & PONDER

Who is this?

Do you recognize the actual account, email address, or phone number, rather than just the displayed name or profile picture? Accounts can be hacked and profiles can be copied.

What do they want?

Money? Personal information? A password? A verification code? Access to your device? If somebody contacts you unexpectedly and immediately wants something valuable, slow down.

Why are they reaching out & does it make sense?

- Why is this ridiculously cheap apartment still available?
- Why does this employer need you to pay before you start?
- Why does your “bank” need the code your bank told you not to share?

When does it need to be done?

Scammers don't want you researching, comparing, asking someone else, or thinking for too long. Any sense of urgency is your cue to slow down.

Where else can I check?

Search independently. Check the official website or app. Contact the person or organization using a number you already have saved (not what’s in the suspicious message). Five minutes of checking can save you considerably more than five minutes of regret.

YOUR BIGGEST THREATS

1 "YOU'D BE PERFECT FOR THIS JOB."

An unexpected job offer lands in your inbox, texts, or DMs. Great pay, easy work, barely an interview. Then you're asked to pay for equipment or training, or share sensitive banking info.

What should you do? Research the company and vacancy independently. Legitimate employers shouldn't need you to send money to get a job.

2 "THIS APARTMENT WON'T LAST LONG."

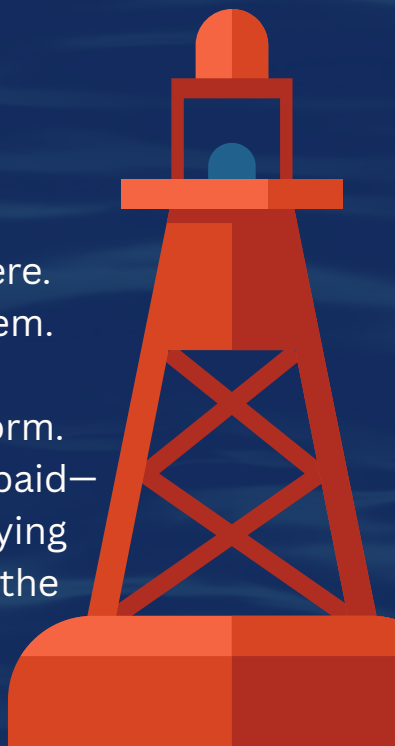
You find a suspiciously affordable apartment. The landlord can't show it to you but needs a deposit now because "several other people are interested."

What should you do? Don't pay before verifying the property, landlord, and agreement, especially if you're pushed to pay before a viewing.

3 "I'LL PAY YOU OUTSIDE THE APP."

You're buying or selling through an online marketplace when someone asks to move the conversation or payment elsewhere. Or, they tell you to wire money to help with moving a large item.

What should you do? Keep chats and payments on the platform. Don't trust screenshots or emails as proof that you've been paid—check your actual bank account. And be extra cautious of paying someone you don't know to move an item. Instead, work out the moving details yourself.





"HEY, IT'S ME. I'VE GOT A NEW NUMBER."

A friend messages from a new number needing money, a code, or urgent help. Or their real account is hacked, so it looks legit.

What should you do? Contact them another way before doing anything. A familiar profile, account, or even voice isn't enough on its own.



"WE HAVE SUCH A CONNECTION."

Dating apps and social media make meeting people easier. They also let scammers build convincing relationships before asking for money, investments, explicit images, or personal info.

What should you do? Be cautious when an online relationship starts involving money or pressure. Never send anything you're uncomfortable sharing, especially if someone threatens or guilts you.



"EVERYONE'S MAKING MONEY FROM THIS."

An investment, crypto scheme, or side hustle promises huge, guaranteed returns. Screenshots show enormous profits. Everyone seems to be getting rich remarkably quickly. Except, potentially, you.

What should you do? Treat guaranteed returns and pressure to invest fast as red flags. Research independently, and never invest just because an influencer or online friend told you to.

WHEN IN DOUBT, STOP AND VERIFY ANOTHER WAY.

OH, CRAP. I FELL FOR A SCAM.

Now what?

Scammers are good at creating urgency, excitement, fear, and trust. Realizing you've been scammed isn't the time for embarrassment. It's the time for damage control.

STEP 1

Stop communicating with the scammer and don't send more money, info, passwords, codes, or photos, even if they claim doing so will solve the problem.

STEP 2



If you sent money or shared payment info, contact your bank, card provider, or payment service immediately.



If you shared a password or code, change it anywhere you've reused it, enable MFA, and check for unfamiliar logins.



If you shared a verification code, change the affected account's password and check for unfamiliar logins or account changes.



If you installed something suspicious, disconnect the device from the internet and get trusted technical help.



If someone is threatening or blackmailing you, stop engaging and save the messages, usernames, payment details, and screenshots as evidence. Don't pay simply because they promise the problem will go away.

STEP 3

Don't be embarrassed. **Tell someone you trust.** Report suspicious accounts through the relevant platform and notify the appropriate organizations or authorities about the fraud.

The quicker you act, the better your chance of limiting the damage.

In the US, report fraud at ReportFraud.ftc.gov and internet crime at ic3.gov.