THE INTERNET SURVIVAL GUIDE

for parents, caretakers & families



What you'll find in this guide:

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

Powered by PHIN

KNOW YOUR SURROUNDINGS

What do these mean?

Kids don't need a degree in cybersecurity and neither do you. But there are a few terms worth knowing.

- **Phishing:** A fake email designed to trick someone into clicking a link, sharing information, or sending money.
- **Smishing:** Phishing by text message.
- **MFA** (multi-factor authentication): An extra security check when you log in, such as a code sent to your phone.
- **Deepfake:** AI-generated video, images, or audio designed to make it look or sound like a real person said or did something.
- **Personal information:** Information that identifies someone, such as their full name, address, school, birthday, phone number, or location.

Teach kids to be suspicious when someone:

🚩 **Asks for secrecy:** "Don't tell your parents."
🚩 **Offers free stuff:** Game currency, skins, prizes, followers, or other rewards in exchange for clicking or sharing something.
🚩 **Asks for information:** Passwords, login codes, personal details, photos, or payment information.
🚩 **Creates urgency:** They need an answer, payment, photo, or action right now.
🚩 **Wants to move the conversation elsewhere:** They ask to move from a game or public platform to a private chat.
🚩 **Makes them uncomfortable:** Something just doesn't feel right, even if they can't explain why.



IMPORTANT: Make sure kids know that telling you quickly is always better than hiding it!

YOUR FAMILY SURVIVAL KIT

For help setting anything up, reach out to IT or a trusted family member or friend.

Support > Punishment. Kids need to know they can tell you when something weird happens online without immediately losing their phone, game, or internet access. **If they're scared you'll be angry, they're more likely to hide a mistake.**

Have a family safe word. AI can imitate voices. Use a word or question to prove it's really you. Even a loud "CA-CAW!" can do the trick.

Use strong, different passwords for every account. If one is stolen, you don't want it unlocking *all* your other accounts. A password manager can create and remember them for you.

Keep phones, tablets, consoles, and apps updated. Most updates fix security weaknesses.

Never share the following about your kids on social media:

- The school they attend
- Real-time photos of where they are and what they're doing
- Their schedule details
- Anything you wouldn't want a stranger to know

Set up MFA. Multi-factor authentication adds another security check when you log in. Use it on important accounts, particularly email, banking, social media, and accounts containing payment information.

Protect purchases. Use parental controls and purchase authentication, and don't leave payment cards unrestricted on children's accounts. 4,800 MegaGems is still real money!

Check privacy settings. Review who can see posts, contact family members, view locations, or access personal information on the apps and games your household uses.



ALWAYS PAUSE & PONDER:

Before anyone in the family clicks, shares, pays, downloads, or replies, ask:

Who is this?

Do we actually know them? A familiar name, photo, or even voice isn't proof.

What are they asking for?

Money? A password? A login code? Personal information? Photos? Be especially suspicious if someone offers a reward in return.

Why do they need it, and does it make sense?

- Does a game really need your password to give you free currency?
- Why does a new online friend need to know where you live?
- Why is a family member suddenly asking for money from a new number?

When does this need to be done?

Scammers don't want you stopping to think or asking somebody else. An urgent request or deadline is a reason to slow down.

How can we verify another way?

Never be embarrassed to ask. Contact them another way, use the official app or website, or ask a trusted adult. **Nobody gets in trouble for checking.**

YOUR BIGGEST THREATS

1 "FREE SKINS! FREE COINS! FREE STUFF!"

A message, video, website, or player promises free game currency, skins, items, followers, or prizes. All your child has to do is click a link, log in, download something, or share a code.

What should you do? If an offer needs a password or login code, it's not a prize. Check the game's official site or app.

2 "DON'T TELL YOUR PARENTS."

Someone your child meets through a game, app, or social platform starts asking personal questions, requesting photos, encouraging secrecy, or trying to move the chat somewhere more private.

What should you do? Make secrecy a family red flag. Kids should know they can end the conversation, block the person, and tell a trusted adult without getting in trouble.

3 "MOM/DAD, I NEED MONEY."

A message or call seems to come from your child, partner, or relative. They have a new number, they're in trouble, and they need money fast. AI can even imitate their voice.

What should you do? Don't send money until you've confirmed it's really them. Hang up and call them back at a number you trust.





"CAN I BUY THIS?"

Games and apps can make real spending feel surprisingly unreal. Kids may also find unofficial sites offering cheaper currency, rare items, or account trades.

What should you do? Require authentication for purchases and don't leave payment cards unrestricted on children's accounts. Only buy digital items through official stores and platforms.



"I NEEEEED MY SOCIAL MEDIA"

Online safety isn't only about scams. Social media can cause mental health challenges by exposing kids to bullying, upsetting content, misinformation, unrealistic comparisons, and communities that encourage harmful behavior.

What should you do? Notice and talk about what they're seeing online, not just how long they're on. Mood changes, secrecy, anxiety about notifications, or distress after going online are reasons to check in.



"JUST POST IT."

Photos and posts can reveal more than you intended. School uniforms can identify where children go to school. Birthday posts reveal sensitive information. Vacation photos can show you're away from home, while backgrounds can reveal addresses or locations.

What should you do? Think before posting. Check what's visible, review privacy settings, and involve kids in what you share about them. Their future 16-year-old self may be less enthusiastic about that adorable bathtub photo.

OH, CRAP. SOMETHING WENT WRONG.

Now what?

Kids click things. Adults click things. Everyone makes mistakes. The important thing is making sure your family tells you quickly enough to do something about it.

STEP 1

Stop communicating with the suspicious person and don't send more money, info, photos, passwords, or codes.

STEP 2



If money or payment information was shared, contact your bank or payment provider immediately.



If someone shared a password, change it anywhere it's been reused and enable MFA.



If something suspicious was downloaded, disconnect the device from the internet and get help.



If inappropriate messages, threats, harassment, or blackmail are involved, save messages, usernames, and screenshots as evidence, block or report the account where appropriate, and involve a trusted family member or friend.

STEP 3

Make this the family rule: nobody gets in trouble for asking for help**. Then report it** to law enforcement and/or the appropriate organization.

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