Module 3:
From passwords to predators: teaching kids safe online habits

A

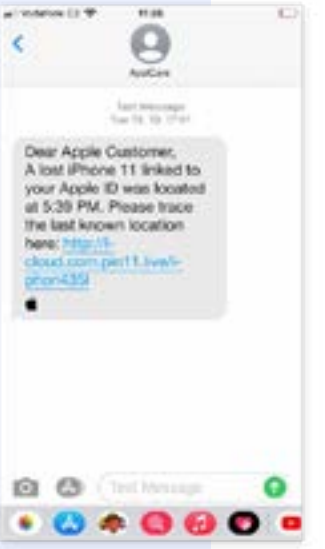
Online safety quiz for caregivers

Test your instincts. Can you spot th real risks?

1. You use a strong, unique password for each account. What is the biggest remaining risk?

- (A) Hackers can still brute-force the password if it's not strong enough.
- (B) If your password manager is hacked, all your accounts are compromised
- (C) Someone could reset your password by answering security questions or gaining access to your email.
- (D) Your ISP (Internet Service Provider) can still see your passwords.

2. What's the most important consideration in determining whether this text message is a scam?



- (A) Apple Support wouldn't text you—they only send emails.
- (B) The link looks similar to Apple's website but is slightly different.
- (C) Major companies never send security alerts via text.
- (D) The message is written in perfect English with no obvious errors.

3. You're setting up a security question for your bank. Which is the worst choice?

- (A) What was your childhood nickname?
- (B) What is your favorite food?
- (C) What city were you born in?
- (D) What was your first car?

A

4. A pop-up appears on your laptop saying your system is infected and you must download a security tool to fix it. What is the safest response?

(A) Download the tool immediately but scan it with antivirus software first.

(B) Close the pop-up and run your existing security software to check for issues

(C) Click the pop-up to see more details before making a decision.

(D) Restart your computer to stop the malware from spreading.

5. You've set up strong passwords and multi-factor authentication (MFA) on your accounts. Which of the following is still a major security risk?

(A) Not using a VPN while on public Wi-Fi.

(B) Auto-filling passwords with your browser's built-in password manager.

(C) Checking email from a shared computer and logging out afterward.

Answers:

1. C: Even with strong passwords, weak security questions or an exposed email account can allow hackers to reset your credentials. Using multi-factor authentication (MFA) helps mitigate this risk.

2. B: Scammers often use links that look close to official ones (e.g., "apple-support.com" instead of "apple.com"). Always check URLs carefully and go directly to the company's website instead of clicking links in texts.

3. C: Birth cities are often public information (on social media, genealogy sites, or public records), making them one of the easiest security questions to guess. The best security questions have answers that aren't easily researched or change over time.

4. B: Legitimate security warnings don't come from pop-ups while browsing the internet. Clicking them often installs malware. Always use your existing security software to verify threats instead of downloading something new from an unknown source.

5. B: Browser-based password managers are more vulnerable to malware and phishing attacks than dedicated password managers. If an attacker gains access to your browser, they can extract saved passwords. Using a separate, encrypted password manager is more secure.

Strong passwords & account security

Why it matters for kids and teens online

Weak passwords are like leaving your front door unlocked—but online. Helping kids create and manage strong passwords is one of the simplest and most effective ways to protect their digital lives, especially as they begin using school portals, games, social media, and email.

What to know

What makes a strong password:

- At least 12 characters long
- A mix of upper- and lower-case letters, numbers, and symbols
- Unique for every account
- Avoids personal information (like names, birthdays, or favorite teams)

Example: L3t$Dance2TheMoon! or G00dM0rning#C0ffee!

Encourage kids to use a **memorable passphrase** or a **password manager** to help keep track of their credentials.

Multi-Factor Authentication (MFA)

MFA adds another layer of security by requiring something beyond just a password—such as a code from an app or a text message. It should be enabled for important accounts such as:

- School portals
- Gaming platforms
- Family email accounts and shared services

Common Mistakes to Avoid

- Reusing the same password for multiple accounts
- Writing passwords on paper or saving them in unsecured apps
- Trusting friends with login information
- Clicking “Save Password” on public or shared devices
- Choosing weak passwords like “123456” or “password”

Teaching Password Safety to Kids

Make the concept relatable and interactive:

- Challenge them to create silly but secure passphrases they can remember
- Use free online sites such as HowSecureIsMyPassword.net
- Role-play scenarios where they must decide what to do if someone asks for their password

Digital Parenthood also provides educational resources and articles for families looking to teach kids about online safety topics >> https://www.aura.com/digital-parenthood

What Parents and Educators Can Do

- Set a strong example by practicing good password habits
- Use Aura’s dashboard to monitor account security, check for breached passwords, and guide kids through best practices
- Regularly review and update account settings together
- Reinforce that passwords are private and should never be shared—even with friends

Source:

UCSB Password Best Practices (https://it.ucsb.edu/general-security-resources/password-best-practices)

A

“Lock it down” dinner with your family

Make cybersecurity a family affair.

Pick a night (maybe once every 3–6 months) to sit down together and change your passwords.

Talk about why password updates matter—like changing your house key if it’s been lost or copied.

Show kids how to update their passwords and check which accounts they use the most.

End with dessert or a movie to make it something they look forward to.

Why it works: Just like brushing teeth or packing lunch, turning online safety into a routine makes it second nature. It also gives parents a regular checkpoint to talk about new apps, websites, or games their kids are using.

Optional secret agent theme

Everyone gets a “Top Secret” mission envelope with instructions like:

- “Create a new password that no villain could guess.”
- “Crack Mom’s riddle to unlock dessert.”
- “Decode this cipher to find the Wi-Fi password.”
- Dress up in sunglasses, trench coats, or whatever’s around the house. Bonus points for walkie-talkies.

Recognizing Online Scams

Scammers know that kids and teens are naturally curious—and often trusting. That makes them prime targets for online phishing schemes, where the goal is to trick someone into giving up personal information, clicking malicious links, or downloading dangerous software.

Phishing doesn't just show up in email anymore. Today's scams often pop up in:

Direct messages on social media

Fake gaming offers

YouTube comments

Texts pretending to be from "school tech support," banks, or even parents

What do phishing messages look like?

Phishing messages are designed to create urgency or curiosity. They often include:

- **Alarming language** like "Act Now!" or "Your account will be deleted"
- **Too-good-to-be-true offers**, such as "You've won a free iPad"
- **Fake login pages** that look almost identical to real ones
- **Strange email addresses or links**—hover over links to preview their true destination
- **Poor spelling and grammar**, which is common in scam messages
- **Requests for sensitive data** like passwords, school ID numbers, or full names

Many phishing attacks are now personalized, using details scraped from social media. This is why even cautious kids may get fooled—especially if the message seems to come from a trusted game or app.

According to the FTC, phishing attacks have steadily increased and are now one of the most common ways scammers target all age groups, including children. In fact, the **Cybersecurity & Infrastructure Security Agency** (CISA) warns that children's digital habits—especially in gaming and chat apps—can make them vulnerable to scams disguised as rewards or "exclusive" offers.

Teach kids to pause before they click

Give them a simple checklist:

- "Do I know who sent this?"
- "Is this link really from who it says it is?"
- "Why are they asking for this information?"
- "Can I double-check this with an adult?"

Even if they're unsure, you can create a rule: If something feels weird—pause, don't click, and ask a grown-up.

Why it matters

Phishing isn't just about emails anymore. Kids can be exposed through any platform that allows messages, including:

- Roblox
- YouTube
- Discord
- Snapchat
- TikTok

And once one account is compromised, scammers often use it to message the victim's friends—making it even more believable.

By helping your child build critical thinking and pattern recognition, you're giving them lifelong digital street smarts.

Sources

Cybersecurity & Infrastructure Security Agency. (n.d.). Protecting children online. CISA. https://www.cisa.gov/news-events/news/protecting-children-online

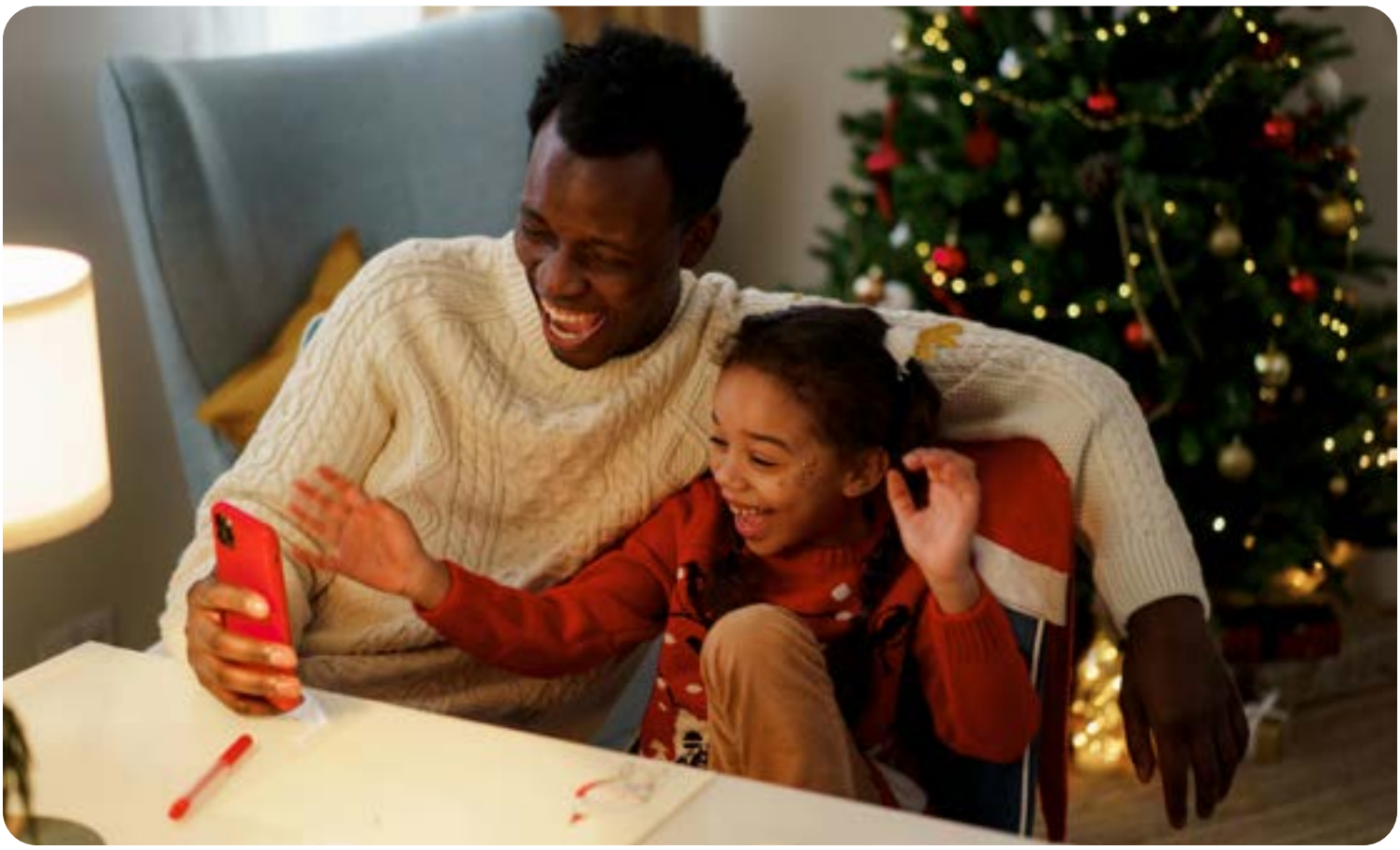
Federal Trade Commission. (2022). How to recognize and avoid phishing scams. FTC Consumer Advice. https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Let me know if you'd like to add more sources (like examples of kid-focused scams or stats on phishing among youth), or if you're ready for this to be compiled into a downloadable doc!

Top 5 things parents and caregivers can do to protect kids' privacy online

Kids don't always realize that the internet never forgets. A simple post or profile update can reveal way more than they think—and once it's out there, it's often out of their control.

But here's the good news: you don't have to be a tech expert to help protect your child's digital privacy. Just taking a few minutes to set the right controls can go a long way in keeping your family safer.



Top 5 privacy moves for parents (that take under 15 minutes)

1. Make social media and gaming accounts private

Go into the app's settings and toggle "private account" ON. This keeps strangers from seeing posts, location tags, and personal info.

Apps like Instagram have "teen supervision" modes that you can enable.

Here are some app-specific guides to help you lock down your child's accounts:

Instagram – Private account and teen account options. Check out the guide.

Facebook – Kids 16 and under are set up with enhanced privacy settings. Check out the guide.

X – Age for participation is 13, but we recommend not allowing due to limited parental controls. Check out the guide.

Roblox - Check out Aura's guide

2. Turn off location sharing

To enhance your child's online privacy and prevent real-time tracking, it's crucial to disable location-sharing features both at the device level and within specific apps like Snapchat, Instagram, and Discord. Here's how you can do it:

iPhone:

1. Open Settings.
2. Tap Privacy & Security > Location Services.
3. Scroll down and select the app (e.g., Snapchat, Instagram).
4. Choose Never or While Using the App to restrict location access.

Android:

1. Open Settings.
2. Tap Location > App permissions.
3. Select the app and choose Deny or Allow only while using the app.

Snapchat:

1. Open Snapchat and tap your Bitmoji in the top-left corner.
2. Tap the gear icon in the top-right to access Settings.
3. Scroll down to Privacy Controls and tap See My Location.
4. Enable Ghost Mode to hide your location from others.

3. Limit who can contact them

In settings, disable DMs (direct messages) from "Everyone." Change it to "Friends Only" or "No One" where possible.

4. Don't use real names in usernames or profiles

Help your child choose usernames that don't include full names, birth years, or school info.

5. Adjust app permissions

On your child's phone, go to Settings → Privacy → App Permissions. Disable access to location, contacts, camera, and microphone unless absolutely necessary.

iPhone (iOS) – Adjust App Permissions

1. **Open Settings**
2. Scroll down and tap **Privacy & Security**
3. Choose the category you want to manage:
    - **Location Services, Contacts, Camera, Microphone,Photos, etc.**
4. Tap each one to see a list of apps using that permission.
5. Tap on an app to change its access (choose **Never, Ask Next Time, or While Using the App**).

Pro tip: Disable permissions for apps that don't need them. For example, a game app doesn't need access to your child's microphone or contacts.

Android – Adjust App Permissions

1. **Open Settings**
2. Tap **Privacy**, then tap **Permission Manager** (or)
3. Go to **Apps** → tap on a specific app → then tap Permissions
3. You'll see categories like:

Location, Camera, Microphone, Contacts

4. Tap each one to see which apps have access.
5. Tap on an app and choose:
    - **Allow only while using the app**
    - **Ask every time**
    - **Don't allow**

Note: The steps might vary slightly depending on your Android version and phone brand, but the general process is similar.

AURA

Want an easier way? Aura's online balance features give parents a simple way to monitor app usage, screen time, and privacy settings—helping kids build safer digital habits without constant surveillance.

Try starting the conversation

Don't just set the settings—talk about them. Kids are more likely to follow privacy guidelines when they understand why they matter.

Try asking:

- "Do you know who can see your posts right now?"
- "What's something about you that should stay private online?"
- "Who would you not want seeing your location?"

Sources
Common Sense Media. (n.d.). Teaching kids to protect their data and privacy online.
https://www.commonsensemedia.org/articles/teaching-kids-to-protect-their-data-and-privacy-online

A

Ai Practice

Meet Jo —
Your teaching partner for online safety

Jo is an AI-powered chatbot designed to help you practice one of the most important skills: talking to kids about staying safe online.
Your job? To guide, support, and empower Jo—just like you would in a real conversation with a child.

Jo can be an elementary, middle, or high school aged and will adapt based on your choices.

How it works

Step 1: Begin your chat

Step 2: Choose an age group

- Elementary (ages 9–11)
- Middle School (ages 12–14)
- High School (ages 15–17)

Step 3: Choose a topic to teach

- Meeting strangers online
- Keeping your information private
- Your online reputation
- Sharing photos and videos online

Step 4: Start the conversation

Test your ability to explain these topics clearly and coach Jo through tough scenarios. The better your responses, the more you'll help Jo make safe, smart decisions.

Goals

Be comprehensive & accurate

Share key online safety concepts using clear, age-appropriate language that kids can understand—and act on.

Teach effectively

Deliver lessons in a way that's engaging and memorable, helping kids retain and apply what they learn in real life.

Encourage critical thinking & ownership

Spark curiosity, invite questions, and empower kids to take responsibility for their digital choices—not just follow the rules.

Talk to Jo

https://talkbetterlab.vercel.app/tbl/scenario/chat/32