

IRVINGTON HIGH SCHOOL PTSA · FREMONT, CA

Safe and Savvy: Cyber Safety for Irvington Families

A parent's playbook for the age of AI

Vaibhav Bhandari · Adjunct Faculty, Merritt College



Welcome. This is an online Zoom meeting, so say how to take part: Zoom reactions (thumbs up) for show-of-hands moments, the chat for votes and short exercises, and the chat or Q&A for questions. Tonight is practical: you will leave with one concrete thing to do at the dinner table. Set the tone: no fear-mongering, no tech jargon.



Vaibhav Bhandari

vitraag.com

A little about me



Adjunct Faculty, Merritt College

Teaching the next generation of tech talent



Software & cybersecurity leader

Healthcare identity, secure messaging at Optum; Microsoft HealthVault



O'Reilly author & patent holder

Contributed to national standards: Direct, Blue Button



Security Engineer

Building products for funded startups; maker and cyclist

Keep to about 60 seconds. Credentials are from vitraag.com/#about; the current title is shown as Security Engineer at your request. The supporting line under it (building products for funded startups, maker and cyclist) is from the site. Suggested personal hook (add your own): why you care as a parent and community member in Fremont.

Today's roadmap

1

Scams: is it really them?

NIST findings, family password, Fremont PD, game malware

2

Privacy and location

The "Meet Maya" exercise

3

Group chats, bullying, AI-faked images

What to do and what to say

4

AI chatbots, controls, family agreement

Controls, password managers, a shared agreement

5

Parenting tips, seven actions, dinner table

Pick one for tonight

Bonus (side note): careers in cybersecurity. If there's interest, we'll do another seminar in more detail.

Walk the five blocks in one breath, and mention the interactive moments (Zoom reactions, chat votes, chat challenges, one action for tonight). Careers are a bonus side note in the backup slides, to be used if there is time or interest. If there is interest, offer a longer follow-up seminar.

Give a thumbs-up if...

REACT

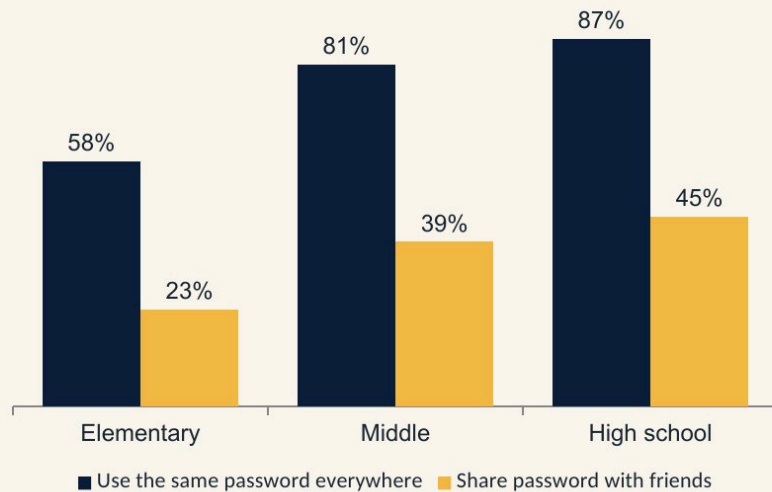
 <p>You use the same password on more than one account</p>	 <p>You got a suspicious text or call this month</p>
 <p>Your teen games on a computer you also use</p>	 <p>Your teen is more tech-savvy than you</p>

Irvington PTSA · Family Cyber Safety

4

Read each prompt, pause for Zoom reactions (thumbs up), quick comment (“you are in good company”). The NIST study found most parents reuse passwords too, so this is a no-shame room. Prompt 3 sets up the Roblox/game-malware story later; prompt 2 sets up the AI voice-scam story.

Teens know the rules. Habits lag behind.



1,505

students (grades 3–12) surveyed by NIST

98% of high schoolers say passwords should be kept private, yet 45% share them with friends.

Key message: kids understand the idea; behavior drifts as they get older and friends matter more. That is normal, which is why a family system beats a lecture. Bar values are from the NIST NRC HACK 2022 slides; values are from slide 11 of that deck (Password Practice: the Good and Bad).

Digital natives still need a guide



Savvy users, not security experts

NIST: skills built from constant use may not go beyond texting, social media and browsing. Teens trust what they find on the web.

47% → 13%

Parents who always help with passwords: elementary vs. high school

We step back just as the stakes rise. Teens still need a safety net, now as a partner.



“We’ve had all those conversations, but it’s been years. I honestly don’t know what he knows at this point.”

Parent of a high schooler, NIST interviews. Parents often underestimate what teens know and care about.

Three NIST findings. (1) Digital natives are heavy users, but NIST found their skills may not extend beyond basics. (2) In the parent survey, 47% of parents of elementary kids always help with password creation vs 13% for high schoolers. (3) In 40 parent/child interviews, parents often underestimated what their kids knew. Bridge: kids are more capable than we think, and more exposed than we think.

It sounds like your kid. It isn't.



1. Grab

A few seconds of a teen's voice from a public video, game stream or story



2. Clone

Cheap AI tools copy the voice. Caller ID can be faked too



3. Panic

"Mom, I'm in trouble. Don't tell Dad. Send money now."

Red flags

- Urgency and secrecy
- Payment by wire, crypto or gift cards
- A "new number" or a stranger "helping"
- Fremont PD: no official demands money right away for a family member's safety
- You can't trust your ears. Verify another way

Tell a short story: a parent gets a call in their child's voice. Scammers need only a few seconds of audio from a public video, story or game stream. The right-hand red flag is from Fremont PD: neither the department nor any US government agency will call and demand money immediately for the safety of a family member. The next slide goes deeper on what Fremont PD tells residents.

Fremont PD: what to know

REACT



Spoofed police calls

Scammers fake caller ID, even the non-emergency line, (510) 790-6800. Officers never call to ask for money. Hang up.



Call your family first

No official demands money right away for a family member's safety. Call your family to confirm they're OK.



Scary texts with your details

A name and address feel personal but are widely available. Don't reply. Call your family.



Fake-check "jobs"

Fremont PD has investigated work-from-home "mystery shopper" cases: deposit a check, buy gift cards. Victims lost thousands.

Report it: Fremont PD online or (510) 790-6800 option 3 · reportfraud.ftc.gov · FBI IC3

Irvington PTSA · Family Cyber Safety | Source: Fremont Police Department, Scams, Fraud & Financial Crimes (fremontpolice.gov)

8

All four cards come from fremontpolice.gov/crime-prevention/scams-fraud-financial-crimes. (1) Fremont PD warns that criminals fake caller ID, including the non-emergency line (510) 790-6800; officers never call from it to request information or solicit money; if you get such a call, hang up. They may also use a real officer's name and claim a missed subpoena, a ticket fine or a tax payment. (2) Neither Fremont PD nor any US government agency will call and demand you send money immediately for the safety of a family member or yourself; call family members first and confirm they are OK; the scammer wants you to react out of emotion. (3) Disturbing-image texts that include a name, address or phone number: that information is generally public or from data breaches; truly specific details (the time you leave for work, a regular sports event) would imply someone is watching. (4) Work-at-home mystery-shopper scams: an official-looking check, instructions to buy gift cards and read out the PIN numbers; the check bounces and the victim loses thousands. Ask for Zoom reactions: who has had a call or text like this? Teen-specific guidance on bullying and AI-faked images comes from ConnectSafely and NCMEC.

Real or scam? Vote in chat.

IN CHAT

A

Call: your teen's voice,
crying

*"I got into an accident.
Don't tell Dad. I need
\$2,000 today."*

B

Call from "Fremont PD"

*"You missed a
subpoena. Pay this fine
now or be arrested."*

C

DM from a classmate's
account

*"Try my new game!
Also, send me the code
you just got."*

D

Work-from-home
"mystery shopper"

*"Deposit this check, buy
gift cards, send us the
numbers."*

The twist: all four are scams. Voice, caller ID and even a friend's account are no longer proof. What is?

Read each scenario aloud (play A in a worried voice). Ask for A, B, C or D in the chat for each (or launch a Zoom poll if enabled), then reveal: all four are scams. A = AI voice clone. B = Fremont PD documents spoofed caller ID that can even show the department's own non-emergency number, with claims of a missed subpoena or ticket fine. C = a familiar account that has been taken over; a login code is the key to the account, so never read one out, even to a friend (Discord's own security page documents malicious downloads, QR codes promising free Nitro and look-alike login sites; it does not specifically cover hijacked friend accounts, so present C as general account-takeover advice). D = the fake-check job scam documented by Fremont PD and the FTC: never pay anyone to get a job. Segue: what is real proof? Something only your family knows.

The Family Password

A shared secret that proves it's really them

IN CHAT

- 1**
Pick it together
Everyone in the family, including grandparents who may be called
- 2**
Make it random
Three unrelated words, like purple-tractor-waffle
- 3**
Keep it offline
Never typed, texted or posted. Say it out loud only
- 4**
Ask, don't offer
The caller must say it. If they can't, hang up and call back

Chat (2 min): how will you pitch this to your teen? Skip pet names, birthdays and anything on social media.

Irvington PTSA · Family Cyber Safety

10

The centerpiece. No tech needed, free, five minutes; works for voice clones, spoofed numbers and “I’m at school, send someone to pick me up” texts. Give everyone two minutes to type in the chat how they would introduce it to a teen (or use breakout rooms if enabled), then read out a few (“a safety game, not a trust issue”). Bad words: pet names, street or school names, birthdays, anything on Instagram or TikTok. Good: three random words or a silly inside joke never posted. Do not post your real word in the chat. Rotate it twice a year or if overheard.

In the news: the “free cheat” trap

BleepingComputer · Aug 3, 2026

Fake Roblox Xeno script launcher pushes infostealer, RAT malware

Steals browser logins, cookies, payment data and crypto wallets. Can watch the webcam.

Malwarebytes · Jun 17, 2026

Roblox developers are losing entire games to malware attacks

One “job offer” file on Discord. Stolen sessions can sidestep two-step login.

TechCrunch · Jul 17, 2026

FBI arrests man accused of using Steam games to drain victims’ crypto wallets

About 8,000 infected devices and \$220K+ stolen. Not Roblox, same trick.

Bitdefender to parents: many Roblox “executors” (cheat tools) are really delivery vehicles for malware.

Read the three headlines aloud. Links: bleepingcomputer.com/news/security/fake-roblox-xeno-script-launcher-pushes-infostealer-rat-malware/ ; malwarebytes.com/blog/scams/2026/06/roblox-developers-are-losing-entire-games-to-malware-attacks ; techcrunch.com/2026/07/17/fbi-arrests-man-accused-of-using-steam-games-to-drain-victims-crypto-wallets/ ; bitdefender.com/en-us/blog/hotforsecurity/roblox-executors-parents-danger-malware (Oct 2025, updated Apr 2026). Be accurate: the Steam case is a different platform, shown to illustrate the same trick (a fun-looking download that drains crypto wallets).

How a cheat reaches Dad's accounts



1. Lure

"Free Robux" or an "undetected" cheat tool on YouTube, Discord or forums



2. Run

Your teen runs the file on the family PC. It looks like the real tool



3. Steal

Saved passwords, login cookies, payment info and crypto wallets from the browser



4. Drain

Anyone logged in on that browser, including Dad's email, shopping or bank, is exposed

Why two-step login isn't enough: stolen login cookies can let attackers in without a password. Sign out of all sessions after an infection.

Walk the four steps with the story: a teen wants an edge in Roblox, runs a "free" tool, and the family computer, which is also logged into a parent's browser, is exposed. Accuracy: published reporting documents these tools stealing browser logins, cookies and payment data, and kids using parents' devices. Say exposed or at risk, not drained, unless you can cite a specific case. Keep it parent-friendly: this is not a Roblox-bashing slide; the official game is fine, the cheat tools are the problem.

Which download is safe?

IN CHAT

A

Roblox from roblox.com or the official app store

B

An “undetected” executor from a YouTube link

C

A free Robux generator a Discord friend shared

Only A. Roblox bans executors, and “free” cheat tools are a common way malware gets in.

Already ran one? Unplug it from the network. From a clean device, change passwords, sign out of all sessions, and call your bank.

Vote in chat for A, B or C, then reveal. Then the “already happened” strip: treat the computer as compromised, rotate passwords from a different clean device, sign out of all sessions, enable 2-step login, watch statements, consider a credit freeze. Reassure: report it to the school/PTSA; no shame, because teens are targeted on purpose.

Meet Maya (she's fictional)

IN CHAT



@maya.k16 · public account

- 1 Go Irvington! Team hoodie photo after the game
- 2 Soccer every Tue and Thu at 4. Come watch!
- 3 Sweet 16 on March 14!!
- 4 New room reveal. House number 2217 visible by the door
- 5 Live story: at Fremont BART right now

Chat challenge (2 min)

- Where does she live?
- Where will she be, and when?
- When is she probably alone?
- What could a stranger guess about her passwords?

Each post is harmless. Together they answer who, where and when. Fremont PD notes that knowing a family's school or sports routine suggests someone is watching.

Give everyone two minutes to post clues in the chat, then reveal: (1) school affiliation in a public profile, (2) a fixed practice schedule = where she will be and when, (3) birthday = date of birth, handy for account recovery and social engineering, (4) a house number in a photo = home address, (5) a live story from a transit station = real-time location. Each post is harmless; together a stranger knows who, where and when. AAP advises limiting location-specific information and reviewing account privacy. Parents: review your own posts too. This is a made-up profile; no real student is depicted. Fremont PD (scams page): general details like a name and address are widely available, but specific routines such as a regular sports event would imply someone has been monitoring a person. Segue: now the settings that fix it.

Privacy and location: fix it together



Audience

- Posts and stories: friends only
- Prune followers they haven't met in person
- Hide the friends list if the app allows



Location

- Snap Map: Ghost Mode ("only me")
- Share live location with trusted people only
- Post outings after you've left



Permissions

- Location: "while using" or off
- Mic, camera, contacts: only if needed
- Parents: review your own posts too

Do it together, not to them: open one app tonight and tour its settings side by side. Five minutes.

NIST tip: help kids own their online presence by setting privacy settings to your comfort level together, and remind them it is OK to limit how and with whom they share. AAP: check privacy settings before using new apps. Snap Map: three audiences (all friends, select friends, only me = Ghost Mode); it updates whenever the app is open, so it is not only when posting. Teens may feel social pressure when their Bitmoji disappears, so talk through it rather than just ordering it. Turning off phone location services is an extra step; also check app-level permissions. Settings change often; test on your own phone before presenting.

Apps parents should know about

REACT



Messaging & video chat

Discord, Kik, WhatsApp, Reddit, Holla, Ask.fm, Hot or Not

Strangers can reach your teen. Many have no identity checks.



Content sharing

Snapchat, TikTok, Live.me

"Disappearing" posts, limited privacy controls, location features.



Secret apps

Calculator%, Whisper

Look harmless. Hide photos and files, or share anonymous secrets.



Dating apps

Badoo, Bumble, Grindr, MeetMe, Skout

Built for adults, but teens are known to fake their age.

Which have you never heard of? Games count too: Roblox, Minecraft, Fortnite and their Discord servers.

The list and categories are from the NIST deck (slide 29), which credits the Pasco County Sheriff's Office, August 2022. The list ages quickly: Omegle appears on the original list but shut down in 2023, so it is left off here. The Games line is an addition and is not on the NIST list. Ask for Zoom reactions: "which of these have you never heard of?". Message: you do not need to ban these; know which ones your teen uses and what the privacy settings are. Refresh with ConnectSafely before the event.

Group chats and cyberbullying

Pew (2022): 46% of US teens have experienced at least one type of cyberbullying.



Don't respond or retaliate

A reaction is often what the bully wants, and hitting back can escalate it



Save the evidence

Screenshot messages, usernames and dates. Never keep explicit images



Block and report

Use the app's block and report tools. It may not end it, but it removes the temptation



Tell a trusted adult

For threats of harm, involve the school and local police

Parents: listen first. You're lucky if they ask for help. Respond thoughtfully, not fast, and banning the app rarely fixes it.

Group chats: bystanders matter. Don't forward a humiliating screenshot. Support the target, report it, tell a school adult.

Verified against ConnectSafely's Parent's Guide to Cyberbullying (updated Jul 26, 2025). Steps for teens: it is not your fault; do not respond or retaliate (retaliating can turn one mean act into a chain reaction); save the evidence; block and report (it probably will not end it, but you will be less tempted to respond); get help; for threats of physical harm call local police with a parent and report to the school; if you see it, do not pass along a mean message. Parent points: you are lucky if your child asks for help, since most do not tell; respond thoughtfully, not fast, because acting publicly can worsen the marginalization; what victims say helps most is being truly listened to; solutions matter more than punishment; banning an app or taking the phone does not solve it, because the interaction continues and a ban can leave the teen left out. Kids may call it drama, so avoid leading with the word cyberbullying. Numbers on ConnectSafely's page: Pew 2022 found 46% of US teens had experienced at least one type of cyberbullying (name-calling 32%, false rumors 22%, unwanted explicit images 17%, explicit images shared without consent 7%); NCES found about 19% of students 12 to 18 were bullied in 2021-22, and 22% of those say it happened online or by text. The group-chat line (leave, do not forward) is a practical addition; ConnectSafely advises not passing along mean messages. Also see connectsafely.org/Sextortion/.

AI-faked images and blackmail

Tell your teen beforehand: a fake still causes real harm, and the target deserves help, not blame.



1. Don't share or send more

No forwarding. Never send more photos to a blackmailer



2. Tell an adult, no blame

Thank your teen for telling you. Stay calm



3. Report it

To the app, and to NCMEC's CyberTipline (report.cybertip.org)



4. Get it removed

takeitdown.ncmec.org: free, for under 18, parents can start it

If someone demands money: don't pay or send more. Keep the threats and account names (not the image), then report.

Sensitive topic: keep your tone calm and matter-of-fact, no graphic detail. From NCMEC's generative AI page: offenders may create an explicit AI image of a child who refused to send a nude, then use it to blackmail the child for more content. NCMEC says report to the CyberTipline (report.cybertip.org), request removal through Take It Down (takeitdown.ncmec.org; anonymous removal requests from participating platforms), and report the content to the platform. NCMEC also offers support: its 24-hour call center is 1-800-843-5678. Do not pay or send more, and keep threats and account details but not the explicit image, are widely given safety guidance rather than NCMEC page text, so present them as general advice. The federal TAKE IT DOWN Act requires platforms to offer removal processes for nonconsensual intimate images; keep claims about its scope general. Resource: connectsafely.org/Sextortion/.

What would you do?

IN CHAT

Your teen says a classmate's AI-edited photo is going around a group chat.

A

Screenshot it and forward it to the parents' group chat

B

Thank them for telling you.
Don't share it. Report it and tell the school

C

Tell them to stay out of it

B. Forwarding spreads the harm, and silence leaves the target alone. Praise your teen for telling you.

Quick vote in chat. Reveal B. Point: your response determines whether your teen tells you next time.

AI chatbots are tools, not friends

Why teens like them

Private, always available, flattering. Common Sense Media: 3 in 4 teens have tried AI companions, 1 in 3 chose AI over a person for a serious talk, 1 in 4 shared personal information.

The risks

- Teens can bond as if it were a real person
- May replace friends, worsening isolation
- Agreeable bots can reinforce unsafe ideas
- Flirty or sexual content can appear

What to do

- Talk openly. Ask what they use it for
- Try it together
- Set clear rules and limits
- Teach: a tool, not a friend or therapist
- Watch for mood changes and pulling away
- Worried? Call your pediatrician

Agree on what stays private: family details, addresses, passwords

Follows AACAP's Facts for Families guide: companions are programs that respond like a helpful friend; appeal is privacy, availability, agreeable and complimentary replies; risks include strong emotional bonds, isolation, reduced social-skills practice, flirtatious or sexual content, and reinforcing unhealthy ideas; AACAP says companions are not considered safe for children and parents should strongly consider restricting or removing access. Model moderate screen use. Be careful to distinguish homework helpers from companion apps. AACAP does not list specific warning signs; the mood and withdrawal items are its general concerns. Common Sense Media research (Talk, Trust, and Trade-Offs): nearly 3 in 4 teens have used AI companions and half use them regularly; about a third have chosen an AI over a person for a serious conversation; about a quarter have shared personal information; its position is that no one under 18 should use these platforms. Ask: "who has heard your teen talk to a chatbot like a friend?"

Practical controls that help



Phones and tablets

Apple Screen Time or Google Family Link: apps, contacts, purchases



Consoles and router

Same controls for games, downloads and who can contact them



App settings

Who can message, public vs. private, purchases, recovery email



Accounts

Password manager, 2-step login, own login for each gamer



Chatbots

Controls vary a lot by app. Check before you allow it



Updates

Automatic updates, antivirus, standard (non-admin) kid accounts

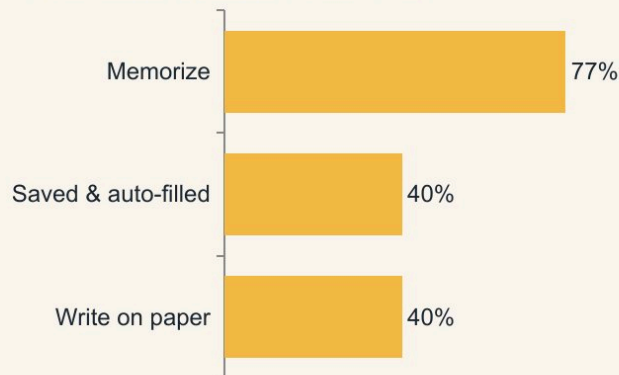
Features vary by device and account setup. The conversation does the real work.

AAP recommends using parental controls for screen time, downloads, contacts and purchases on routers, phones, tablets, consoles, social media accounts and school devices, and turning off autoplay and notifications. Bitdefender (Roblox executors guide): standard accounts without admin rights for kids, updates, real-time antivirus, 2-step login on Roblox, email and payment accounts. NIST: your home is not the only place kids go online, so settings alone are not enough. Chatbot controls: they vary widely; some provide parental settings, many have none. Product controls change often, so check them on your own phone before demonstrating. Password managers are the next slide.

Let a manager remember for you

ACTION #2

How parents keep track of passwords



NIST survey of 265 parents; multiple answers allowed. Only 12% change passwords by account type; 53% only when needed.



One unique password per account

NIST found parents have fewer passwords than accounts, so reuse creeps in.



One strong master password

Add 2-step login to the manager itself. It is the only one to remember.



Autofill is a fake-site alarm

A manager won't fill a login on a look-alike site, a useful warning sign.

Apple Passwords (iCloud), Google Password Manager, 1Password, Bitwarden: any works. Pick one this month.

This is action 2 of the seven (protect accounts, keep login codes private). The NIST deck has no password-manager slide; the data is NIST's parent password survey: 77% memorize, 40% write on paper, 40% saved and auto-filled, 53% change only when needed. Name the options without endorsing one: Apple Passwords (iCloud Keychain) if the family is on iPhone, Google Password Manager (in Chrome and Android), and dedicated apps such as 1Password or Bitwarden that work across devices; several offer family plans or shared groups for shared logins like streaming or Wi-Fi. The recommendation itself is general best practice, not NIST's. Demo idea: show the autofill prompt on your phone, and note it will not fill on a look-alike site. Remind parents to protect the manager with a strong master password and 2-step login. Kids: younger children rely on family to create and remember passwords, so set it up together; teens can run their own.

A family media agreement

YOUR TURN

1. Screen-free times and places: dinner, homework, bedtime
2. One screen at a time
3. Notifications and autoplay off
4. Check privacy settings before any new app
5. Make room for sports, reading, friends, hobbies
6. Adults follow the same rules, dinner included

Review it each school year and every summer. Teens help write it.

Our Family Agreement

Screens off at _____

Phones charge in _____

If something goes wrong, I will _____

We review this on _____

Signed: parents _____ teens _____

The six items come from AAP's "How to Make a Family Media Use Plan": screen-free times and places, one screen at a time, turn off autoplay and notifications, check privacy settings, make room for other activities, model healthy habits yourself. AAP: every family is different; discuss the rules with your kids; include a plan for every family member including parents; review at the start of the school year or on summer and holiday breaks. AAP has little teen-specific guidance on this page; involving teens in writing the rules is the key teen point. The sample fill-in card is the presenter's idea. Suggest a free printable from [healthychildren.org](https://www.healthychildren.org) (search "Family Media Plan").

Parenting digital natives



Stay current

Keep up with online risks and dangers



Keep a resource list

One set of trusted sites for the whole family



Walk the talk

Get your own security habits right first



Start early

Make good online behavior second nature



Talk about good and bad

Friendships and fun, plus threats and risks



Think critically

Question what you find online, in email, chat and social

These six points are NIST's "Parenting Digital Natives" slides (27-28). Also from NIST's "Youth Cybersecurity and Privacy Education" slide: reinforce good perceptions early (kids' understanding of passwords is reasonably accurate), promote concrete understanding (kids describe why passwords matter only vaguely), and bridge the gap between knowledge and behavior (e.g., sharing passwords with friends). Make the "walk the talk" point lightly: NIST found parents reuse passwords too.

Seven actions: pick one

YOUR TURN

<p>1</p> <p>Verify unusual requests independently</p> <p>Hang up, call back, use the family password</p>	<p>2</p> <p>Protect accounts and keep login codes private</p> <p>Password manager: iCloud, Google, 1Password</p>	<p>3</p> <p>Check opportunities before sending money or information</p> <p>Fake internships, giveaways, free cheats</p>	<p>4</p> <p>Review audiences, location and app permissions together</p> <p>Profile, Snap Map, mic and camera</p>
<p>5</p> <p>Refuse to amplify bullying or intimate images</p> <p>Don't forward, don't pile on</p>	<p>6</p> <p>Agree on AI use and healthy device boundaries</p> <p>Chatbots are tools, not friends</p>	<p>7</p> <p>Make asking for help easy, and have a response plan</p> <p>"You won't be in trouble for telling me"</p>	<p>Tonight I will...</p> <p>Pick ONE. Post it in the chat.</p>

Irvington PTSA · Family Cyber Safety

25

Walk the seven quickly (about 10 seconds each), tying each to something from tonight: 1 = family password and voice clones; 2 = password manager, 2-step login, never read out a login code; 3 = fake jobs, giveaways and free cheats; 4 = the Maya exercise; 5 = group chat and AI-image slides; 6 = chatbots and the media agreement; 7 = “you won’t be in trouble for telling me”, with a plan: who to call, what to screenshot, how to report. Then give 60 seconds: each parent types the number of the ONE action they will do tonight in the chat. Ask people to type the number in chat.

At the dinner table

TONIGHT

Pick one to ask tonight

- “What’s the weirdest message you’ve ever gotten?”
- “If I called you in trouble, how would you know it was me?”
- “Show me your favorite game. Where do cheats and mods come from?”
- “What do you use AI chatbots for?”
- “If a mean or fake photo of someone got shared, what would you do?”
- **Stay calm. Just saying “no” rarely works**

Trusted resources

ConnectSafely

connectsafely.org

Family Online Safety Institute

fosi.org

iKeepSafe

ikeepSAFE.org

StaySafeOnline

staysafeonline.org

Bookmark one tonight.

Give parents 30 seconds to type in the chat the one question they will ask this week. Conversation tips draw on NIST’s Internet Safety and Security Tips for Parents: remain positively engaged, just saying no rarely works, make it a teachable moment, support good choices as they show competence. ConnectSafely adds: listen first, and it is a good sign if your teen asks for help. The four resources are from the last slide of the NIST deck; NIST suggests keeping a ready collection of reputable resources for the family.

Start with one tonight

- 1 Set the family password together
- 2 Tour one app's privacy and location settings
- 3 Fill in the family media agreement

Questions?

If there's interest, we'll do another seminar in more detail.

Vaibhav Bhandari · vitraag.com · Adjunct Faculty, Merritt College

Land the three actions, then take questions. If time is short, end here and hang around afterwards for questions.

Backup slides

Bonus side note: careers in cybersecurity. Use if there is time or interest.

Backup section: the bonus careers side note. Use it if there is time or interest.

Bonus: a career worth knowing

500,000+

unfilled U.S. cybersecurity jobs, per CyberSeek

Many students never see it as an option, because they picture a hoodie-wearing hacker.

Side note. If there's interest, we'll do another seminar in more detail.

Myth vs. reality

~~Only for coders and math whizzes~~

Also law, policy, teaching, investigating, communications

~~Hackers in dark rooms~~

Protecting hospitals, schools, cars and power grids

~~Solo work~~

Teams of analysts, builders and communicators

Keep this light. Tie back: the skills tonight (skepticism, verifying, protecting people) are the same skills of a cyber career. 500,000+ figure is from the NICE webinar deck citing CyberSeek/CompTIA 2025. As an adjunct at Merritt, share one line on the students you see.

Try it, explore it, get started



Try it (free)

- TryCyber.us: hands-on challenges
- Cyber clubs and competitions at school
- National Cyber League, NCAE Cyber Games



Explore roles

- CyberSeek.org: jobs and career maps
- Technical and non-technical paths
- Start from interests, not job titles



Start at Merritt

- AS or certificate: Infrastructure or Applications Security
- Free CyberCamp for high schoolers
- BangNull club competes in the National Cyber League

Tip for teens: ask “what problem do I want to protect people from?” before “what job do I want?”

Keep it light. TryCyber, CyberSeek, National Cyber League and NCAE Cyber Games are from the NICE webinar deck. Merritt details are from merritt.edu/cybersecurity: AS degrees and Certificates of Achievement in Infrastructure Security and in Applications Security (AS about two years, classes on Fridays, with internships and labs); CyberCamp is a free two-week introductory course for middle schoolers, high schoolers and adults; the BangNull Cybersecurity Club, founded in 2014, competes in the National Cyber League; Merritt students placed in the top 2.8% in the Spring 2025 National Cyber League rankings; the program holds an annual Cybersecurity Career Day. Merritt is in Oakland (12500 Campus Drive). CyberCamp dates and eligibility are on the Merritt page; check them before promising anything to families.