

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





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

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.

Give a thumbs-up if...

REACT



You use the same password on more than one account



You got a suspicious text or call this month

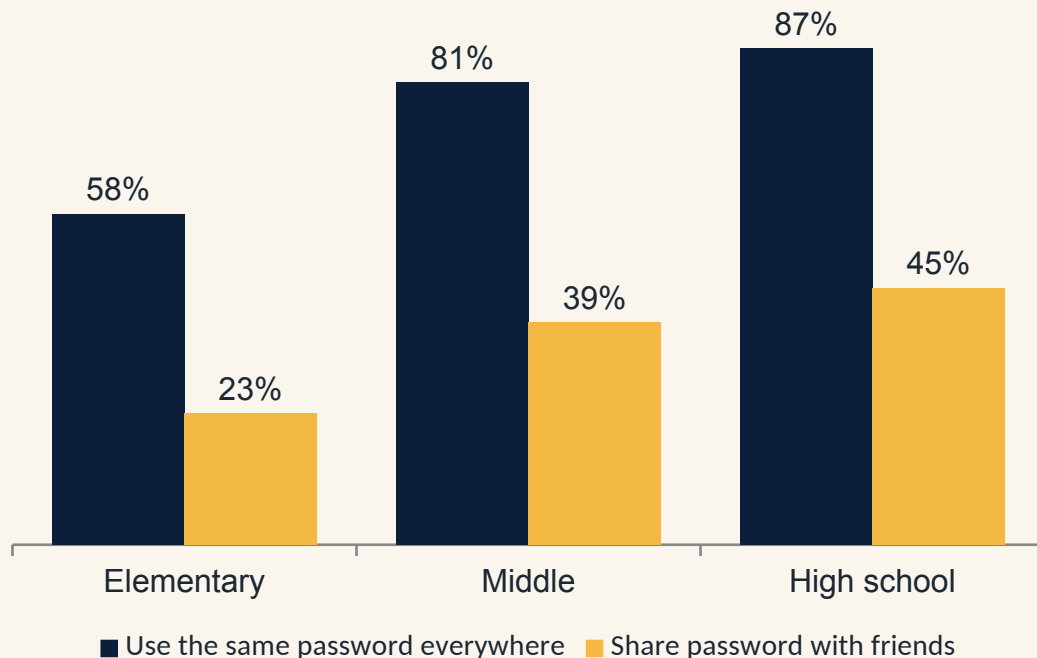


Your teen games on a computer you also use



Your teen is more tech-savvy than you

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.

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.

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

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

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?

The Family Password

IN CHAT

A shared secret that proves it's really them

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.

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.

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.

Which download is safe?

IN CHAT



Roblox from roblox.com or the official app store



An “undetected” executor from a YouTube link



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.

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.

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.

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.

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.

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.

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.

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

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

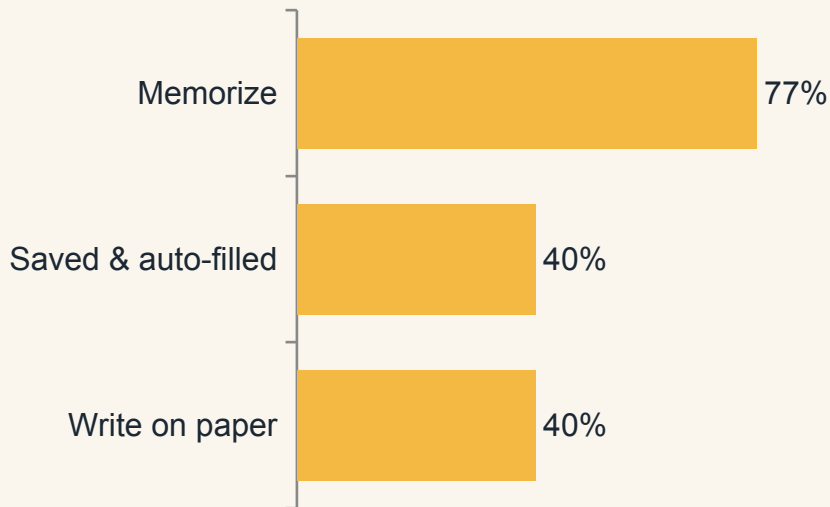
Automatic updates, antivirus, standard (non-admin) kid accounts

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

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.

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 _____

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

Seven actions: pick one

YOUR TURN

1

Verify unusual requests independently

Hang up, call back, use the family password

2

Protect accounts and keep login codes private

Password manager: iCloud, Google, 1Password

3

Check opportunities before sending money or information

Fake internships, giveaways, free cheats

4

Review audiences, location and app permissions together

Profile, Snap Map, mic and camera

5

Refuse to amplify bullying or intimate images

Don't forward, don't pile on

6

Agree on AI use and healthy device boundaries

Chatbots are tools, not friends

7

Make asking for help easy, and have a response plan

"You won't be in trouble for telling me"

Tonight I will...

Pick ONE. Post it in the 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.

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

Backup slides

Bonus side note: careers in cybersecurity. Use 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

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?”