LANCASTER

CONNECTED WITHOUT COMPROMISE

TEEN SAFETY GUIDE

Privacy, Accounts, Scams, Relationships, AI & Recovery

A practical guide for teens, families, educators, and youth professionals

LANCASTER SOLUTIONS LLC SAFETY EDUCATION TEAM

Secure. Fast. Built to grow.

CONNECTED WITHOUT COMPROMISE

A TEENAGER'S GUIDE TO INTERNET SAFETY

A practical guide for ages 13–18, families, educators, and youth-serving professionals

PRIVACY • ACCOUNT SECURITY • SCAMS • AI • RELATIONSHIPS • RECOVERY

Prepared by the Lancaster Solutions LLC Safety Education Team

Research and resources reviewed through July 2026

EXPANDED LEARNING EDITION

Connected Without Compromise: A Teenager's Guide to Internet Safety

Second Publication Edition - July 2026

Prepared and edited by the Lancaster Solutions LLC Safety Education Team.

Facts, laws, school rules, platform settings, and reporting processes change. Use the update center before relying on a platform-specific instruction.

Updates and corrections: Connected Without Compromise update center

Accessibility: this edition uses structured headings, descriptive navigation, high-contrast text, and tagged-PDF export. Readers who need another format may contact the publisher through the Lancaster Solutions LLC website.

ISBN: not assigned for this website educational edition.

Publication and Safety Note

This book is educational. It is not legal advice, medical advice, or a substitute for emergency services. Laws, school policies, platform rules, and reporting requirements vary by location. The resource section focuses primarily on the United States and includes international starting points where possible.

If someone is in immediate physical danger, call emergency services. In the United States, call 911. If you or someone you know is in emotional crisis or at risk of self-harm, call or text 988. If a minor is being sexually exploited online, contact the National Center for Missing & Exploited Children CyberTipline and local law enforcement. Detailed steps appear in the emergency resources section.

All scenarios in this book are fictional composites. They are designed to reflect realistic situations without describing any identifiable person.

Contents

The Series Safety Backbone

Every response framework in the Connected Without Compromise series maps to the same five actions. The mode-specific acronym helps you remember the context; the backbone helps you act even when you forget the acronym.

1. PAUSE OR LEAVE - Stop the interaction, stream, lobby, payment, upload, or automated action.

2. PRESERVE EVIDENCE - Save usernames, links, timestamps, messages, transaction records, and report numbers without redistributing harmful material.

3. SECURE ACCESS - Protect the primary email, accounts, devices, sessions, recovery methods, and payment tools.

4. TELL A USABLE ADULT - Bring in a calm adult or qualified professional who can help without making disclosure feel like punishment.

5. REPORT AND FOLLOW UP - Use the correct platform, school, bank, child-safety, crisis, or law-enforcement route, then record what happens next.

Memory line: Stop the pressure. Save the facts. Secure the door. Bring in help. Keep following up.

Fast Path: The Essential Teen Safety Route

The full edition is designed as a reference. A reader who needs the highest-value skills first can use this shorter path:

1. Start Here If Something Is Happening Right Now.

2. The Two Safety Loops.

3. Chapter 2: account security and recovery.

4. Chapter 5: scams and verification.

5. Chapters 7-8: grooming, sextortion, and image abuse.

6. Chapter 11: harassment, doxxing, and threats.

7. Chapters 14-15: incident response, reporting, and helping a friend.

8. Appendix C: pocket action cards.

Complete the remaining chapters when they match your life, schoolwork, relationships, or current risks. Safety does not require reading every page before taking the next safe step.

Introduction for Parents and Educators

The internet is not a separate world teenagers visit after school. It is where homework is assigned, friendships deepen, teams organize, art is shared, games are played, identities are explored, and opportunities appear. It is also where manipulation can travel at the speed of a notification.

That combination creates a difficult job for adults. You are expected to protect young people without isolating them, guide them without spying on them, and respond to crises involving technologies that may not have existed when you were their age. Rules alone cannot solve that problem. A teenager who believes that admitting a mistake will automatically cost them their phone, friendships, privacy, or freedom may hide the exact situation in which adult help is most important.

The central idea of this book is **connection without surrender**. Teenagers can participate fully in digital life while keeping control of their accounts, attention, personal information, boundaries, and choices. Adults can support that control by building trust, rehearsing response plans, and treating online harm as real harm rather than as evidence that a young person is irresponsible.

The Most Important Protective Factor Is a Usable Adult

A usable adult is not perfect. A usable adult is someone a teenager can approach before a problem becomes a catastrophe. That person listens long enough to understand what happened, separates safety from punishment, and takes action with the young person rather than immediately taking over.

Consider two possible responses when a teenager says, “I sent something I regret, and now they are threatening me.”

The first response is: “How could you do that? Give me your phone. You are never using that app again.”

The second response is: “I am glad you told me. You are not in trouble for asking for help. We are going to slow this down, save evidence, stop contact, and report it together.”

The second response does not excuse risky behavior. It creates the conditions for disclosure, evidence preservation, and safety. Federal law-enforcement and child-protection organizations repeatedly emphasize that shame and fear can keep young victims silent, while early disclosure can stop continuing harm.[11][19]

Replace One-Time Lectures With Repeated Practice

Online safety works more like fire safety than like a single school assembly. Knowing that smoke is dangerous is not the same as knowing where the exits are. A strong family or school plan rehearses practical questions:

- Who are the three adults a student can contact at any hour?
- What happens if an account is stolen?
- How can screenshots be saved without spreading harmful content?
- Which school staff member handles harassment reports?
- What should a teen do if a friend mentions suicide or self-harm?
- How will adults respond if a teen admits to clicking a scam link, sending money, or sharing an intimate image?

Practice lowers the amount of thinking required during panic. That matters because scammers, bullies, and exploiters deliberately create urgency, embarrassment, secrecy, and fear.

Safety Is Not the Same as Surveillance

Adults sometimes respond to online risk by demanding every password, reading every conversation, or installing invisible monitoring tools. There are situations in which close supervision is justified, especially for younger teens, immediate safety concerns, or known exploitation. But routine secret surveillance can damage trust, expose sensitive conversations, and teach young people to hide rather than seek help.

A more sustainable approach is transparent, age-appropriate oversight. Explain what will be monitored, why, for how long, and what would allow more independence. Focus on high-risk areas—unknown contacts, financial transactions, disappearing messages, location sharing, late-night use, and sudden behavioral changes—rather than treating every private conversation as suspicious.

The goal is not to know everything a teenager says. The goal is to make sure they know what to do when something unsafe happens.

Use This Book as a Conversation Tool

Each chapter contains a fictional scenario, a summary, a practical checklist, and discussion questions. Adults can read the book alongside teens, assign selected chapters, or use the scenarios in advisory periods, health classes, technology courses, youth groups, and counseling settings.

Avoid turning every discussion question into an interrogation. Ask what the character could do, what makes the situation difficult, and which response would feel realistic. Teenagers often discuss a fictional person more honestly than they discuss themselves. That distance can open a door.

A Trauma-Informed Response to Online Harm

When a teenager experiences cyberbullying, grooming, sextortion, identity theft, stalking, or image-based abuse, their reactions may include panic, anger, numbness, shame, sleep disruption, school

avoidance, or sudden withdrawal. These reactions do not prove guilt or dishonesty. They may be signs that the person feels trapped.

A trauma-informed response begins with five messages:

1. **I believe you.**
2. **This is not your fault.**
3. **You are not alone.**
4. **We will take one step at a time.**
5. **You will have a voice in what happens next whenever safety allows.**

Do not force a young person to repeatedly retell a traumatic event to multiple adults. Record essential facts once, preserve evidence carefully, and involve trained professionals where appropriate.

What This Book Does Not Do

This guide does not claim that every stranger is dangerous, every platform is harmful, or every mistake creates permanent ruin. Fear-based messaging can make teens dismiss adults as unrealistic. Most online interactions are ordinary. Many are positive. The purpose of safety skills is not to eliminate participation; it is to improve judgment, reduce preventable risk, and make recovery faster when prevention fails.

A teenager does not need perfect judgment to deserve protection. Adults do not need perfect technical knowledge to provide it. Both need a shared plan.

Introduction Summary

- Online life is part of real life, not a lesser version of it.
- Trust increases the chance that teenagers will disclose dangerous situations early.
- Safety plans should be practiced before they are needed.
- Oversight should be transparent, proportionate, and focused on risk.

- A calm, non-shaming first response can preserve evidence and protect a young person.

Adult Readiness Checklist

- ☐ I can name at least two reporting resources for online exploitation.
- ☐ The teens in my care know they can report a mistake without automatic punishment.
- ☐ We have a written plan for stolen accounts, harassment, and threatening messages.
- ☐ I understand the privacy and safety settings on the main platforms they use.
- ☐ I know the school or organization contact for bullying and safety concerns.
- ☐ I will preserve evidence before deleting accounts or resetting devices.
- ☐ I know when to contact 911, 988, NCMEC, law enforcement, or a specialized hotline.

Discussion Questions for Adults

1. What consequences in our home or school might unintentionally discourage early reporting?
2. How can we distinguish reasonable privacy from dangerous secrecy?
3. Which adult in our community would a teenager actually contact at midnight?
4. What would a calm first ten minutes look like after a serious online disclosure?

A Note to Teen Readers

You do not need to become suspicious of everyone to become safer online. You need a few habits that give you time, evidence, options, and backup.

The internet often rewards speed. Reply now. Post now. Buy now. Prove it now. Send the picture now. Join the call now. Real safety usually begins with the opposite move: pause.

A pause is not weakness. It is how you take control back from people and systems that benefit when you react before thinking.

This book will not tell you to "just get off the internet." That would be like teaching road safety by saying never leave the house. It will show you how to use digital spaces without handing over more than you intended.

You will learn how to:

- protect accounts without memorizing dozens of impossible passwords;
- recognize scams that look like messages from friends, schools, employers, or game companies;
- understand what apps collect and what posts reveal;
- spot grooming, coercion, and fake intimacy;
- respond to sextortion without paying or sending more material;
- verify images, videos, and claims in an AI-generated world;
- protect your mental health without blaming yourself for persuasive design;
- help a friend without trying to become their therapist, investigator, or rescuer;
- recover when something goes wrong.

One rule appears throughout this book: **mistakes do not cancel your right to help**.

You might click a link. You might trust someone who lied. You might send something private. You might post while angry. You might reuse a password. You might freeze when you wish you had acted. None of those things make abuse, fraud, threats, or humiliation your fault.

Your responsibility is to take the next safe step. The other person is responsible for choosing to exploit, threaten, deceive, or harm.

Keep the emergency resource pages somewhere you can reach without unlocking this entire book. Consider sharing them with a friend. You may never need them. Someone you care about might.

SECTION

Start Here If Something Is Happening Right Now

You do not need to finish this book before asking for help. Use the route below that matches what is happening. Then go to the named chapter for the full plan.

Someone is threatening to share an intimate image

Do not pay, send more, bargain, or threaten back. Save the account name, profile link, messages, payment request, and threat without forwarding the image. Tell a trusted adult now. Report through the platform and NCMEC CyberTipline. Use Take It Down when the image was taken before age 18. See Chapter 8.

Your account was taken over

Start with the primary email that resets the other accounts. Use the official app or site, change reused passwords, sign out unknown sessions, restore recovery information, and turn on strong MFA. Warn contacts through another channel. See Chapters 2 and 14.

You clicked a scam link, sent money, or gave away a code

Leave the message. Open the real account directly. Change exposed passwords, contact the bank or payment service immediately, and preserve receipts and messages. Tell an adult if money, identity information, school, or work is involved. See Chapters 5 and 14.

Your address, school, routine, or live location was posted

Move to a safe place if there is an immediate threat. Save the URL, username, time, and screenshots. Do not start a public fight. Tell a

trusted adult, school safety contact, platform, or law enforcement based on the risk. See Chapters 4, 11, and 14.

A friend says they may hurt themselves or cannot stay safe

Treat it as real. Keep contact while bringing in an adult or emergency support. In the United States, call or text 988; call 911 for immediate danger. Do not promise to keep a life-threatening secret. See Chapters 13 and 15.

Your phone warns that an unknown tracker is moving with you

Go to a safe public place, save the alert and map, and involve a trusted adult. Do not confront a suspected person alone. In an abusive situation, use a safer device to get specialized safety-planning help before making changes that could alert the person. See Chapter 4.

The Two Safety Loops

You do not need fifty rules under pressure. Memorize two loops: one for decisions and one for emergencies.

PAUSE BEFORE YOU TAP P - Pressure: What emotion or deadline is pushing me? A - Ask: What am I being asked to give - access, money, an image, location, secrecy, or attention? U - Use another channel: Leave the message and open the real app, site, or contact yourself. S - Source: Who started this, and what independent evidence confirms it? E - Exit and engage backup: Stop the interaction and involve a trusted person when the risk is bigger than you.

WHEN HARM IS ALREADY HAPPENING STOP - Do not pay, send more, argue, or delete in panic. SAVE - Preserve usernames, links, dates, messages, and report numbers without redistributing harmful content. TELL - Break secrecy with a trusted adult or qualified helper. REPORT - Use the platform and the correct school, provider, hotline, or law-enforcement channel.

Your Three Rights Online

- You have the right to pause, even when someone says the decision cannot wait.
- You have the right to say no without proving love, loyalty, maturity, courage, or trust.
- You have the right to ask for help after a mistake. A mistake never creates permission for someone else to exploit you.

How to Make These Lessons Stick

Reading can make information feel familiar without making it easy to recall during stress. This edition repeatedly asks you to close the book, retrieve a skill from memory, make a choice in a realistic scenario, say the words out loud, and revisit the idea later. Retrieval practice and

spaced review consistently improve long-term retention compared with repeated reading alone.[27][28]

Use the book in short rounds:

1. Read one chapter or one section, not the entire book in a single sitting.

2. Before reading the summary, answer the Close the Book questions from memory.

3. Say the sample script out loud. Words rehearsed before pressure are easier to use during pressure.

4. Complete the 60-Second Drill on your real device or account.

5. Return one day and one week later and explain the memory anchor to another person.

6. Use the part checkpoints without looking back. The goal is not a perfect score. The goal is a faster safe first move.

> **THE STANDARD FOR SUCCESS** You do not need to remember every setting, law, or hotline. You need to recognize pressure, create time, preserve options, and reach the right backup.

PART I

Control Your Digital Space

Connection grows stronger when control, judgment, and recovery skills grow with it.

CHAPTER 1

Your Online Life Is Real Life

Maya is sixteen and takes photos for her school newspaper. Her profile is not “public public,” as she puts it. Only friends can see her posts. She assumes that means her information stays inside a circle she controls.

One Friday, a classmate she barely knows asks why she is always at the same coffee shop after school. Maya never posted the shop’s address. Then she looks at her recent photos: the mural behind her, a bus-stop number reflected in a window, the name of a dance studio across the street, and a caption that says, “Here every Friday until my ride gets off work.”

No single detail seemed private. Together, they formed a map.

Privacy Is Control, Not Invisibility

Privacy does not mean hiding everything. It means deciding what different people can know, when they can know it, and what they can do with that information.

You already use privacy boundaries offline. A teacher may know your grades but not your private group-chat jokes. A close friend may know who you like but not your family’s financial information. A coach may know your injury history but not your phone passcode. Online platforms blur those boundaries because one post can be copied, searched, forwarded, analyzed, and combined with other information.

The important question is not only, “Is this secret?” It is also:

- Who can see this?
- Who can copy it?
- What else could it be combined with?
- How long might it remain available?
- Could it identify my routines, relationships, school, home, or vulnerabilities?

Your Digital Environment Has Layers

Think of your online life as four connected layers.

Layer 1: What You Intentionally Share

This includes posts, comments, videos, usernames, profile photos, bios, playlists, wish lists, livestreams, and public game activity. It is the easiest layer to notice because you press “post.”

Layer 2: What Other People Share About You

Friends tag you. Teams post rosters. Schools publish event photos. Family members announce birthdays. Someone records a group video in which your location or conversation appears. You do not fully control this layer, but you can influence it by asking people not to tag your location, reviewing tags before they appear, and reporting content that violates consent or platform rules.

Layer 3: What Apps and Devices Collect

Apps may collect device identifiers, approximate or precise location, contacts, search activity, purchases, ad interactions, voice recordings, usage patterns, and information from other services. The FTC has warned that major social-media and video-streaming companies have engaged in extensive collection, retention, and monetization of user data, with particular concerns for teens.[4]

You may never type this information into a post. It can still become part of your digital profile.

Layer 4: What Others Infer

Inference is the part people underestimate. A collection of likes may suggest your interests, beliefs, insecurities, or spending habits. Late-night activity may reveal sleep patterns. A public sports schedule may reveal when your home is empty. Repeated backgrounds may reveal where you live. A streak of posts about a breakup may tell a manipulator when you are lonely and easier to approach.

An inference can be wrong and still affect you. Recommendation systems, advertisers, scammers, bullies, and strangers may act on what they think they know.

Build a Personal Threat Model

"Threat model" sounds technical, but it means answering three ordinary questions:

1. **What am I protecting?**
2. **Who or what could interfere with it?**
3. **Which protections are worth the effort?**

Your answers may include:

- accounts and saved photos;
- your physical location;
- private conversations;
- family information;
- money or game items;
- your reputation;
- your ability to contact friends;
- your mental space and attention.

The likely threats are not always movie-style hackers. They may be an ex who still knows your passcode, a friend borrowing your phone, a scammer using a fake school account, an app collecting more data than you realized, or someone screenshotting a private story.

A useful threat model is realistic. You do not need military-level security for a meme account. You do need strong protection for your main email because it can reset many other accounts.

The Email Account at the Center of Everything

Your primary email is often the control room for your digital life. It receives password-reset links, account alerts, purchase receipts, school messages, and login codes. If someone controls it, they may be able to

take over social accounts, cloud storage, shopping profiles, and financial services.

Treat your main email differently from low-value accounts:

- use a unique password or passkey;
- turn on strong multifactor authentication;
- review recovery phone numbers and backup addresses;
- save recovery codes somewhere secure;
- check recent login activity;
- remove old devices and third-party access;
- use a device lock that others cannot guess.

Boundaries Work Best Before Pressure Starts

A boundary is easier to keep when you decide it before someone challenges it. Examples include:

- “I do not share live location with people I have not met offline.”
- “I do not send verification codes to anyone.”
- “I do not move a conversation to disappearing messages just because someone asks.”
- “I do not share passwords with dating partners.”
- “I do not post someone else’s private message without permission.”
- “I do not argue with anonymous accounts after midnight.”

Boundaries are not proof that you distrust people. They are rules that prevent a moment of pressure from deciding your safety.

The Screenshot Test—With Limits

Adults often say, “Never post anything you would not want on a billboard.” That advice is too broad to be useful. People need private spaces, humor, vulnerability, and experimentation.

A better version is the **screenshot test**:

Before sending something sensitive, ask what would happen if the recipient saved it, misunderstood it, lost their account, or showed one

other person. This does not mean you should never trust anyone. It means digital trust should include the possibility of copying.

The screenshot test also applies to other people's content. Having the technical ability to capture something does not create permission to share it.

Scenario: Maya Rebuilds the Map

Maya reviews her account with a friend. They search her username while logged out, check tagged photos, and look at old public comments. She removes her school abbreviation from her bio, turns on tag review, disables precise location for the photo app, and stops posting from the coffee shop in real time.

She does not delete photography. She changes the timing and context. She posts after leaving, crops identifying details when appropriate, and keeps a separate public portfolio with no routine information.

That is privacy in practice: not disappearing, but choosing.

Make It Stick

MEMORY ANCHOR Pieces become a map.

Pressure Test

You post a photo from a team bus. The image shows your school logo, a route number, the time, and the caption "same ride every Thursday." A new follower asks whether the bus always stops near your house.

A. Answer because the route is already public.

B. Delete the comment only and keep posting the route in real time.

C. Save the message, block or restrict the account, review what the photo reveals, and delay future routine posts.

BEST FIRST MOVE C. The risk is not one secret fact. It is the repeated pattern. Reduce the pattern, not your entire online life.

60-Second Drill

Open one profile while logged out or in a private browser window. In sixty seconds, list every clue a stranger could use to identify your school, schedule, close relationships, usual locations, or recovery answers. Change the highest-impact clue first.

Say It Out Loud

I share the memory after I leave. I do not publish a live map of where I am and when I am alone.

Close the Book: Recall

Before reading the summary, cover the page and answer from memory:

1. Define privacy without using the word “secret.”
2. Name the four layers of a digital environment.
3. Which single account can reset the most other accounts?

Chapter 1 Summary

- Privacy is the ability to control access, context, timing, and use.
- Small details can combine into a surprisingly accurate picture of your life.
- Your primary email deserves the strongest protection because it can reset other accounts.
- A personal threat model helps you focus on realistic risks instead of fearing everything.
- Pre-decided boundaries are easier to enforce during pressure.
- Privacy is compatible with creativity, friendship, and public participation.

Chapter 1 Safety Checklist

- ☐ Search my name and main usernames while logged out.
- ☐ Review what my profile reveals about school, routines, family, and location.
- ☐ Check tagged posts and enable tag or mention review where available.

- ☐ Identify my most important account and strengthen it first.
- ☐ Remove old recovery emails, phone numbers, devices, and app connections.
- ☐ Write three boundaries I will use before a high-pressure situation occurs.
- ☐ Ask before posting private information about someone else.

Chapter 1 Discussion Questions

1. Which pieces of information seem harmless alone but risky when combined?
2. What is the difference between privacy and secrecy?
3. Which account would cause the most damage if someone took it over?
4. What online boundary would be hardest to explain to a close friend or partner?
5. How can a person participate publicly without sharing live routines?

CHAPTER 2

Lock the Door—Passwords, Passkeys, and Account Recovery

> ***QUICK RECALL - Do not look back:*** *What can small public details become when they are combined?* ***Check:*** *A map of routines, relationships, and vulnerabilities.*

Eli is seventeen and works weekends at a grocery store. He uses one "good" password with small variations: the same phrase, a different number, and sometimes an exclamation point. It feels efficient. He can remember every version.

Then a gaming forum announces a data breach. Within a day, someone logs into Eli's email, resets his social-media password, and messages his contacts asking for money. The attacker did not guess every variation. Automated tools tried credentials from the breached site on other services—a common method called credential stuffing.

The weak point was not that Eli's password lacked a symbol. It was that one breach opened several doors.

Length and Uniqueness Beat Password Acrobatics

Modern password guidance has changed. The current NIST Digital Identity Guidelines emphasize length, reject forced mixtures of character types as a general requirement, discourage routine password changes without evidence of compromise, and support password managers. For passwords used alone as a single factor, NIST's 2025 standard requires a minimum of fifteen characters for covered systems and recommends allowing at least sixty-four.[1]

You are not operating a federal system, but the lesson is useful:

- make passwords long;
- make each important password unique;
- avoid predictable personal information;
- use a password manager when possible;
- change a password when it is exposed or reused—not merely because a calendar says so.

A long passphrase can be easier to remember than a short jumble. Do not use examples printed in books or online. Create your own unrelated words or let a password manager generate a random value.

Why Reuse Is So Dangerous

Suppose you use the same password for a low-value fan forum and your email. The forum may have weaker security. If it is breached, attackers may obtain usernames, email addresses, and password data. Even when passwords are stored in protected form, weak or common passwords may be cracked.

Attackers then test those credentials against email, social media, shopping, gaming, school portals, and payment services. They do not need to target you personally. Automation makes one reused password valuable.

Use unique credentials at minimum for:

1. primary email;
2. school or work account;
3. banking or payment services;
4. cloud photo and file storage;
5. major social-media accounts;
6. gaming accounts with purchases or valuable items.

Password Managers: One Strong Vault, Many Unique Keys

A password manager stores encrypted credentials and can generate unique passwords. It reduces the need to memorize dozens of secrets. NIST notes that password managers and password generators can increase the likelihood that users choose stronger, distinct passwords.[1]

A manager still needs protection:

- Use a strong, unique master password or passphrase.
- Turn on multifactor authentication for the vault.
- Keep the app and operating system updated.
- Understand account-recovery options before you need them.
- Do not approve a login you did not initiate.
- Avoid storing the master password in an unlocked note or chat.

Built-in managers from major operating systems and browsers may be appropriate for many users. Dedicated managers may offer additional sharing, family, auditing, and cross-platform features. The best option is one you can secure and consistently use.

Passkeys: A Different Kind of Login

A passkey uses public-key cryptography rather than sending a reusable password to a website. In plain language, your device proves it has a secret key while the website stores a matching public key. The secret itself is not typed into a login form.

Passkeys are often unlocked with a device PIN, fingerprint, or face recognition. They can be significantly more resistant to phishing because they are tied to the legitimate site or app. NIST recognizes WebAuthn/FIDO2 methods as phishing-resistant when correctly implemented.[1]

That does not make passkeys magical. Your device account, recovery process, screen lock, and synced-key account still matter. Use a strong device PIN, review trusted devices, and maintain recovery options.

Multifactor Authentication: More Than One Proof

Multifactor authentication, or MFA, requires more than one type of proof. CISA recommends enabling MFA because a stolen password alone is then less likely to be enough.[2]

Common methods, from generally stronger to generally weaker, include:

- security keys or passkeys using FIDO/WebAuthn;
- authenticator apps that generate time-based codes;
- push approvals with number matching or clear login details;
- text-message codes;
- email codes.

Any MFA is usually better than password-only access. Phishing-resistant options such as passkeys or hardware security keys are stronger because a fake site cannot simply ask you to type the code and relay it. NIST notes that manually entered one-time codes are not considered phishing-resistant, even though they still add protection.[1]

The MFA Fatigue Attack

Jordan receives six login prompts while playing a game. He taps “deny” twice, ignores three, and approves the sixth just to make them stop. The prompt was not a glitch. Someone already had his password and was trying to wear down his attention.

Never approve an unexpected login. If prompts repeat:

1. deny them;
2. change the password from a trusted device;
3. review active sessions and sign out others;
4. check recovery information;
5. report the activity to the service;
6. tell a trusted adult if the account affects school, money, or safety.

Recovery Is Part of Security

People often configure security for the happy path—when the phone works, the password is remembered, and the account is accessible. Real security includes losing a device, changing a number, or being locked out.

Review:

- backup email addresses;
- recovery phone numbers;
- saved recovery codes;
- trusted devices;
- family recovery contacts, where supported;
- account legacy or inactive-account settings;
- the process for replacing a lost security key.

Store recovery codes somewhere separate from the device they unlock. A printed copy in a secure location may be reasonable. A photo of recovery codes in the same cloud account they recover is less useful if that account is compromised.

Device Locks Matter

A strong account password does not help if someone can open your unlocked phone and change settings. Use a device PIN or passcode that is not your birthday, graduation year, jersey number, address, or a simple pattern visible from across a room.

Biometrics are convenient, but they are not secret in the same way a password is. Your face and fingerprints exist in the world. Use biometrics as part of a well-configured device, not as an excuse for a weak fallback PIN.

Be cautious about sharing device passcodes with friends or partners. Sharing may feel like trust, but it creates access to messages, photos, password resets, location history, and financial apps. Healthy relationships do not require permanent access to each other's devices.

Account Security Drill

Choose one major account and complete this drill:

1. Sign in through the official app or a bookmark you created—not a message link.
2. Change any reused password.
3. Enable the strongest MFA option available to you.
4. Save recovery codes.
5. Remove devices you do not recognize.
6. Review third-party apps with access.
7. Turn on login alerts.
8. Check whether messages, forwarding rules, or filters were changed.

Email forwarding rules deserve special attention after a compromise. An attacker may create a rule that quietly sends copies of messages or hides security alerts.

Scenario: Eli Contains the Takeover

Eli's first instinct is to post, "I was hacked." Instead, he starts with email recovery because it controls the other accounts. From a clean device, he changes the email password, removes an unknown recovery address, signs out all sessions, enables an authenticator app, and saves backup codes.

He then resets his social accounts through official apps, warns contacts not to send money, and reports the fraudulent messages. He checks payment methods and game purchases. Finally, he replaces every variation of the breached password with generated unique passwords.

He cannot undo the breach. He can stop one breach from becoming a long chain.

Make It Stick

MEMORY ANCHOR One important account, one unique key.

Pressure Test

Six sign-in prompts appear while you are busy. The sixth says it came from a nearby city, and you are tempted to approve it just to stop the alerts.

A. Approve once and change the password later.

B. Deny it, open the account directly, change the password, sign out other sessions, and review recovery details.

C. Turn off notifications so the prompts stop.

> **BEST FIRST MOVE** B. Repeated prompts can be an MFA-fatigue attack. The attacker may already know the password and needs only one approval.

60-Second Drill

Secure your primary email now: confirm its unique password or passkey, strongest available MFA, recovery phone and email, trusted devices, recovery codes, and forwarding rules. Do not postpone the recovery-code step.

Say It Out Loud

I did not start this login. I am denying it and checking the account through the official app.

Close the Book: Recall

Before reading the summary, cover the page and answer from memory:

1. Why is password reuse more dangerous than a short password on only one low-value account?
2. Which MFA methods are phishing-resistant?
3. Where should recovery codes be stored?

Chapter 2 Summary

- Password reuse allows one breach to spread across many accounts.
- Long, unique passwords are more useful than predictable complexity tricks.

- Password managers make unique credentials practical.
- Passkeys and FIDO/WebAuthn security keys can resist many phishing attacks.
- Unexpected MFA prompts should always be denied and investigated.
- Account recovery, trusted devices, and backup codes are part of security.
- Your primary email and device lock deserve priority.

Chapter 2 Safety Checklist

- ☐ My primary email has a unique password or passkey.
- ☐ I use a password manager or another secure system for unique credentials.
- ☐ MFA is enabled on email, school, financial, cloud, gaming, and major social accounts.
- ☐ I know which MFA method each account uses.
- ☐ I saved recovery codes outside the account they recover.
- ☐ I reviewed logged-in devices and third-party app access.
- ☐ My phone PIN is not based on public personal information.
- ☐ I will never share a login code or approve an unexpected prompt.

Chapter 2 Discussion Questions

1. Why is a unique password more important than adding one symbol to a reused password?
2. What are the advantages and risks of a password manager?
3. Why can an authenticator code still be phished?
4. Which recovery method would fail if your phone disappeared today?
5. How can couples or close friends show trust without sharing passcodes?

CHAPTER 3

Privacy Without Disappearing

> ***QUICK RECALL - Do not look back:*** *Which account should receive your strongest protection?* ***Check:*** *Your primary email, because it often resets everything else.*

Nia downloads a photo-editing app because everyone in her art class uses the same filter. The app asks for access to all photos, contacts, microphone, precise location, and nearby devices. Nia taps “allow” each time because the requests appear during setup and she wants to reach the editing screen.

The app only needed one photo.

Permission Prompts Are Decisions, Not Obstacles

Apps often request permissions at the exact moment you are excited, distracted, or in a hurry. That design makes “allow” feel like the button that continues and “do not allow” feel like the button that breaks the app.

Treat every permission as a trade:

- What feature needs this information?
- Does it need access once, while I use the app, or all the time?
- Can I choose selected photos instead of my entire library?
- Can I enter a contact manually instead of uploading my address book?
- What happens if I say no?

Start with the least access and add more only when a feature clearly requires it.

High-Impact Permissions

Photos and Videos

Full-library access may reveal screenshots, identification documents, health information, private images, school schedules, and photos of other people. Use “selected photos” or “add photos only” when available.

Contacts

Uploading contacts exposes information about people who did not choose the app. It can also help platforms build relationship maps. Ask whether finding friends is worth sharing your entire address book.

Microphone and Camera

Messaging, video, and creative apps may reasonably need these permissions while in use. A flashlight or wallpaper app probably does not. Check for unexpected background access.

Location

Choose approximate rather than precise location when the feature does not require exact positioning. Prefer “while using the app” over continuous access. Location deserves its own chapter because it can reveal routines and physical safety information.

Notifications

Notifications are not only a convenience. They are access to your attention and sometimes to private content on your lock screen. Disable unnecessary alerts and hide sensitive previews.

Accessibility, Device Administration, and VPN Profiles

These permissions can be powerful. Accessibility access may allow an app to read screen content or control interactions. Device-administrator or management profiles may change security settings. VPN profiles can route network traffic. Do not approve them for an unknown app because a video promised free followers, game currency, or a “secret mode.”

Privacy Settings Are Not One-Time Settings

Platforms add features, change defaults, and introduce new sharing categories. Review privacy at least every few months and after major app updates.

Check:

- who can see posts, stories, friends, and followers;
- who can message, call, tag, mention, remix, duet, or add you to groups;
- whether search engines can link to your profile;
- whether contacts can find you by phone number or email;
- whether read receipts and activity status are visible;
- whether the app suggests your profile to contacts;
- whether ads are personalized using off-platform activity;
- whether old posts remain public;
- whether your likes, playlists, purchases, or game activity are visible.

Privacy settings reduce exposure. They do not create a guarantee. A follower can still copy content, lose an account, or show a screen to someone else.

Data Minimization: Give Less by Default

Data minimization means providing only what is necessary for the task.

You can practice it by:

- leaving optional profile fields blank;
- using a month and day without a public birth year;
- avoiding school names in public bios;
- using a separate public contact address for creative work;
- not connecting every app to the same social login;
- limiting quizzes that ask about pets, family, childhood, and preferences;
- deleting accounts you no longer use;

- removing old posts that reveal current security answers or routines.

Some “fun” questions overlap with account-recovery questions: first pet, childhood street, mother’s maiden name, favorite teacher. Security questions are weak because answers may be researched, guessed, or socially engineered. Where possible, use random answers stored in a password manager rather than truthful public facts.

Private Browsing Is Not Invisibility

Private or incognito mode mainly prevents the browser from saving local history, cookies, and form data after the session. It does not automatically hide activity from websites, schools, employers, internet providers, account services, or network administrators.

It is useful when:

- signing into an account on a shared device;
- searching for a surprise gift;
- reducing local traces on a device you are authorized to use;
- testing what a page looks like while logged out.

It is not a cloak. Do not rely on it for safety from an abusive person who controls the device or account. In those situations, use a safer device and contact a specialized service for planning.

Public, Private, and Pseudonymous Accounts

Different accounts can serve different purposes:

- a public portfolio for art, music, sports, or professional interests;
- a private personal account for known friends;
- a pseudonymous account for a hobby or support community.

Separation can reduce accidental mixing, but it only works if you avoid linking clues. Reused usernames, identical profile photos, the same writing style, shared contact information, or cross-posted images can connect identities.

Pseudonymity can protect exploration and participation. It can also create false confidence. People may still infer identity from details, metadata, social connections, and patterns.

Deleting Is Useful Even When It Is Not Perfect

You may hear that “the internet is forever.” That phrase can create hopelessness. Copies and archives can persist, but deletion still matters. Removing a post reduces easy access, search visibility, future resharing, and the amount of data available for casual discovery.

Do not let the possibility of a screenshot stop you from cleaning old content, closing unused accounts, revoking app access, or submitting removal requests.

Scenario: Nia Runs a Permission Audit

Nia opens her phone’s privacy dashboard. The editing app has used location in the background eleven times. She changes photo access to selected images, denies contacts and precise location, and disables lock-screen previews.

She finds three games connected to an old social account and removes them. She deletes an abandoned anonymous Q&A profile that still shows her school mascot. She does not become invisible. She reduces the number of companies and strangers holding unnecessary pieces of her life.

Make It Stick

MEMORY ANCHOR Least access first.

Pressure Test

A popular editing app asks for all photos, all contacts, microphone access, precise location, accessibility control, and a VPN profile before showing the first screen.

A. Allow everything because the app store approved it.

B. Start with selected photos only and deny permissions that do not match the feature.

C. Use private browsing so the permissions cannot matter.

> **BEST FIRST MOVE** B. Permission prompts are access decisions. App-store presence and private browsing do not erase unnecessary device access.

60-Second Drill

Open the phone privacy dashboard by permission category. Choose one high-impact permission - location, photos, contacts, microphone, accessibility, or device management - and remove every app that cannot explain why it needs that access.

Say It Out Loud

I will enable that permission when a feature actually needs it, not because setup tries to rush me.

Close the Book: Recall

Before reading the summary, cover the page and answer from memory:

1. What can full photo-library access reveal beyond ordinary photos?
2. What does private browsing actually hide?
3. Why can uploading contacts expose other people?

Chapter 3 Summary

- Permission prompts should be evaluated, not automatically accepted.
- Photos, contacts, location, microphone, accessibility, and device-management access deserve special caution.
- Privacy settings change and should be reviewed regularly.
- Data minimization reduces what can be exposed, sold, inferred, or misused.
- Private browsing mostly affects local browser history; it does not make activity anonymous.

- Deleting old content and accounts still reduces risk, even when copies may exist.

Chapter 3 Safety Checklist

- ☐ Review app permissions by category, not one app at a time.
- ☐ Change full photo access to selected-photo access where possible.
- ☐ Remove location, microphone, camera, or contact access that lacks a clear purpose.
- ☐ Hide sensitive notification previews on the lock screen.
- ☐ Review who can message, tag, mention, call, and add me to groups.
- ☐ Delete unused accounts and revoke old third-party connections.
- ☐ Separate public work from personal information when useful.
- ☐ Remember that private browsing is not anonymity.

Chapter 3 Discussion Questions

1. Why do apps ask for permissions during setup rather than later?
2. Which permission can reveal information about other people, not just you?
3. When is a pseudonymous account helpful, and what can connect it to a real identity?
4. Why is deleting old content still worthwhile if screenshots may exist?
5. What information do you provide only because a field is available?

CHAPTER 4

Location, Photos, and the Clues You Did Not Mean to Share

> ***QUICK RECALL - Do not look back:*** *What permission rule reduces unnecessary exposure?* ***Check:*** *Start with the least access and add only what a feature needs.*

Sam is sixteen and volunteers at an animal shelter. On Saturday morning, Sam posts a photo of a new puppy with the caption, “Alone on intake duty until noon.” The shelter’s name is not visible. The post does show a street sign through the window, an employee badge reflected in a metal bowl, and a location sticker added automatically by the app.

A follower replies, “I could come keep you company.” Sam has never met that follower.

Location Is More Than a Pin on a Map

Location information can be exact, approximate, inferred, or historical.

- **Exact location** may come from GPS, Bluetooth beacons, nearby Wi-Fi networks, or a live-location feature.
- **Approximate location** may be estimated from an internet address or nearby cell towers.
- **Inferred location** may come from signs, landmarks, weather, school logos, transit routes, shadows, reflections, or event schedules.
- **Historical location** appears in old posts, photo libraries, maps timelines, fitness routes, and saved check-ins.

The NSA's updated 2026 guidance on limiting location-data exposure emphasizes that mobile devices create location information through several systems and that users should reduce unnecessary location sharing, app access, wireless signals, and account exposure.[5]

You do not need to eliminate location services. Navigation, emergency functions, rides, weather, and family coordination can be valuable. The goal is to make location sharing intentional.

Live Location Changes the Risk

A photo posted after you leave is different from a livestream announcing that you are alone right now. Live information gives another person a chance to act while the situation is still true.

Use extra caution with:

- being home alone;
- walking or waiting alone;
- a workplace closing shift;
- an empty house during vacation;
- a school practice ending time;
- a hospital, shelter, counseling office, or protected address;
- a friend's home or family situation;
- protest, political, religious, or support-group attendance;
- a routine route repeated every day.

Delay is a powerful privacy tool. Post after leaving. Share the memory without broadcasting the opportunity.

Photo Metadata and Cloud Copies

Digital photos can contain metadata, including date, time, device information, editing history, and sometimes coordinates. Many social platforms strip some location metadata when an image is uploaded, but you should not assume every service does. Sending an original file through email, cloud storage, shared albums, or certain messaging systems may preserve more information.

Before sharing a sensitive image:

1. review its location details in the photo app;
2. remove location metadata if the device offers that option;
3. consider sharing a screenshot or exported copy when appropriate;
4. check the background and reflections;
5. confirm that the image does not expose someone else's address, schedule, school, identification, or private documents.

Screenshots may remove some original metadata, but they can create other clues. They may show usernames, notifications, time, battery level, tabs, or private messages.

Fitness Apps and Routine Maps

Running, cycling, and fitness apps can create detailed route maps. Repeated routes may reveal home, school, work, or a person's usual time alone. A route that begins and ends at the same private address is especially revealing.

Use privacy zones or trim the start and end of routes where available. Limit who can view activities. Avoid public challenges that reveal exact routine times. Remember that group activities may expose multiple people.

AirTags, Trackers, and Unwanted Location Monitoring

Small trackers can help find keys and bags, but they can also be misused. Modern phones may warn about an unknown tracker moving with you. Do not ignore repeated alerts.

If you receive a tracker warning:

- move to a safe, public place if you feel at risk;
- do not confront a suspected person alone;
- save screenshots of the alert and map;

- follow the phone's instructions to make the tracker sound or identify it;
- contact a trusted adult, school safety official, or law enforcement as appropriate;
- if an abusive partner or family member may be monitoring you, use a safer device to contact a specialized domestic-violence or dating-abuse service before making changes that could alert them.

The safest response depends on the relationship and immediate danger. Evidence and safety planning may matter more than immediately destroying the device.

Location Sharing With Friends and Family

Location sharing can increase safety when it is mutual, limited, and understood. It can become controlling when someone demands constant access, checks every stop, punishes delays, or treats a disabled location as proof of betrayal.

Healthy sharing answers these questions:

- Who can see it?
- Is it temporary or continuous?
- What is the safety purpose?
- Can either person stop without retaliation?
- Does the app reveal location history as well as current location?
- What happens if the account is compromised?

A partner who says, "If you loved me, you would let me track you all the time," is not asking for proof of love. They are pressuring you to surrender a boundary.

Scenario: Sam Changes the Audience and the Timing

Sam saves the threatening reply, blocks the follower, tells the shelter manager, and removes the location sticker. The shelter updates its volunteer rules: no live posts identifying who is alone, no visible badges or intake records, and no location tags during a shift.

Sam still posts puppy photos. The posts go up after the shift, with backgrounds checked and location removed. The lesson is not “never share.” It is “do not make a public announcement out of a temporary vulnerability.”

Make It Stick

MEMORY ANCHOR Post the memory, not the opportunity.

Pressure Test

You are waiting alone after practice. A story shows the field name, dark parking lot, and “ride is forty minutes late.” A follower you do not know offers to pick you up.

A. Accept because the follower knows your teammates.

B. Keep chatting while you wait so someone knows where you are.

C. Save the message, contact a trusted adult or coach, move near safe adults, and remove the live post.

BEST FIRST MOVE C. Live location plus temporary vulnerability creates an opportunity. A familiar-looking profile is not transportation safety.

60-Second Drill

Review who can see your live location and activity maps. Turn off one continuous share you no longer need, create privacy zones for fitness routes, and set a rule for delayed posting when you are alone or away from home.

Say It Out Loud

I do not publish where I am alone in real time. I will post after I am safe and gone.

Close the Book: Recall

Before reading the summary, cover the page and answer from memory:

1. Name three ways location can be inferred without GPS.
2. What can a reflection reveal?

3. When can immediately disabling a tracker increase danger?

Chapter 4 Summary

- Location can be exact, inferred, or reconstructed from patterns.
- Live posts create different risks from delayed posts.
- Photo backgrounds, reflections, metadata, and screenshots can reveal more than the subject.
- Fitness routes can expose home addresses and routines.
- Unknown-tracker alerts should be documented and taken seriously.
- Location sharing is healthy only when it is voluntary, limited, and safe to stop.

Chapter 4 Safety Checklist

- ☐ Set most apps to “while using” or no location access.
- ☐ Use approximate location when exact location is unnecessary.
- ☐ Review photo location before sharing original files.
- ☐ Check backgrounds, mirrors, windows, badges, documents, and screens.
- ☐ Delay posts that reveal I am alone or away from home.
- ☐ Make fitness activities private or hide route endpoints.
- ☐ Review who has continuous access to my location.
- ☐ Know what to do if my phone reports an unknown tracker.

Chapter 4 Discussion Questions

1. Which clues in a photo can identify a place without a location tag?
2. When does location sharing support safety, and when does it become control?
3. Why might immediately disabling a tracker be unsafe in an abusive situation?
4. What routines are visible through your posts, stories, maps, or activity status?
5. How could a school club share event photos without exposing students’ routines?

SECTION

PART I CHECKPOINT

The Photo, the Login, and the Ride Home

This checkpoint combines privacy, account security, permissions, and location. Do not search for a perfect answer. Decide what protects the most important thing first.

> **RULE** Choose the safest first move, not the action that solves everything at once.

1. The Photo

A friend posts a group photo while you are still at an empty practice field. Your school, car, and “waiting alone” caption are visible. What is the safest first move?

2. The Login

While trying to remove the post, you receive an unexpected login approval. What do you do before changing social-media settings?

3. The Editing App

The photo editor requests all photos and precise background location to blur the license plate. What permission level is reasonable?

4. The Ride

A mutual follower offers a ride and says your friend can confirm they are safe. What information do you verify and through whom?

5. The Boundary

Write one sentence that lets you ask friends not to post your live location without turning it into a personal accusation.

Answer Key and Reasoning

1. Ask the friend to remove or edit the live post, move near safe people, and contact your ride or another trusted adult. The live vulnerability matters more than winning an argument in comments.

2. Deny the approval and secure the primary email or affected account through the official app. An attacker with the account can undo privacy changes.

3. Selected-photo access is enough. Precise background location does not match the task.

4. Verify the person through the friend using a separate known channel, and still use an adult-approved transportation plan. A mutual connection is not a safety guarantee.

5. Example: “Please wait until we leave before posting me or the location. I want the memory online, not a live announcement that I am here.”

Teach It Back

Explain the checkpoint to another person in sixty seconds. Use the memory anchors, not the chapter titles. If you cannot explain the first move without looking, review only the section you missed and try again tomorrow.

PART II

Spot Manipulation

Connection grows stronger when control, judgment, and recovery skills grow with it.

CHAPTER 5

Scams, Phishing, and Social Engineering

> ***QUICK RECALL - Do not look back:*** *What is safer than posting while you are still alone at a location?* ***Check:*** *Post after leaving; share the memory, not the opportunity.*

Jordan receives a direct message from an account using his assistant coach's name and school logo. The message says the team's new uniform order failed and every player must confirm a payment account within twenty minutes. A link opens a page that looks like the school portal.

Jordan notices one strange detail: the coach usually calls him by his last name. This message says, "Dear student athlete."

He almost ignores the feeling because the page looks professional.

A Scam Is Usually a Story With a Deadline

Scammers do not begin with malware or payment instructions. They begin with a story designed to create emotion:

- **fear:** your account will close;
- **urgency:** act in ten minutes;
- **authority:** this is your principal, coach, bank, police department, or employer;
- **reward:** you won, were selected, or can earn easy money;
- **curiosity:** look what someone posted about you;
- **helpfulness:** a friend needs a code or emergency payment;
- **romance:** someone finally understands you;
- **embarrassment:** private information will be exposed;
- **scarcity:** only three items remain;

- **belonging:** everyone in the group already did it.

The story changes. The pressure pattern stays similar.

The FTC describes phishing as emails or texts that imitate trusted organizations and try to steal passwords, account numbers, or other personal information, often by claiming a problem, suspicious login, refund, invoice, or urgent need to click.[3]

The Pause-Leave-Verify Method

When a message creates pressure, use three steps.

1. Pause

Do not click, reply, call the provided number, open the attachment, send a code, or make a payment. Take one breath and name the emotion being used.

2. Leave

Exit the message. Open the official app from your home screen or use a bookmark you created. Do not use the contact information in the suspicious message.

3. Verify

Contact the person or organization through a known channel. Ask a coach in person. Call the number on the back of a payment card. Type the school's known address. Start a new message to the friend instead of replying to the request.

Verification is not rude. A real person with a real emergency will understand why you checked.

Links Can Lie in Several Ways

A link's visible text may not match its destination. A domain may use a misspelling, extra word, unusual ending, or confusing subdomain.

Compare:

- `school.edu` versus `school-helpdesk.com`

- `accounts.example.com` versus `example.accounts-check.com`
- `paypaI.com` using a capital “I” instead of a lowercase “l”
- a shortened link that hides the destination
- a QR code that prevents you from seeing the address before scanning

The important part of a web address is the registered domain immediately before the ending such as `.com`, `.org`, or `.edu`. Attackers may place a trusted name elsewhere in a long address.

Do not assume a padlock icon means the site is honest. It means the connection is encrypted to that site. Scam sites can also use encryption.

Attachments, Documents, and “View Shared File” Messages

A document may ask you to enable macros, install a viewer, sign in again, or grant cloud access. Treat unexpected shared-file notices like unexpected links.

Verify with the sender through a separate channel, especially when the file involves:

- scholarships;
- job applications;
- invoices or refunds;
- disciplinary records;
- team rosters;
- shared photos;
- legal threats;
- urgent school assignments.

Keep software set to update automatically. The FTC recommends current security software, automatic device updates, MFA, and backups as layers against phishing consequences.[3]

Verification Codes Are Keys

A common scam begins when someone says:

- “I accidentally sent my code to your phone.”
- “I need the code to prove you are real.”
- “Send the code so I can add you to the team account.”
- “The buyer-protection service needs your six digits.”
- “Vote for me by sending the code you receive.”

The code may be authorizing a login, password reset, phone-number transfer, payment, or account registration. Do not share it. Legitimate support workers generally do not need you to read them a code sent with a warning not to share it.

Money-Mule and Fake-Check Scams

Scammers may recruit teenagers to receive and move money. The pitch can sound like a job, favor, scholarship task, art commission, mystery-shopping assignment, or social-media sponsorship.

Common versions:

1. Someone sends a check for more than expected.
2. Your bank makes some funds appear available.
3. The sender asks you to return the extra amount, buy gift cards, or pay a “vendor.”
4. The check later proves fake.
5. The bank removes the deposit, but the money you sent is gone.

Another version uses payment apps or cryptocurrency and asks you to forward funds for a commission. Even if you did not create the fraud, moving stolen money can create serious consequences.

The FTC warns that young adults are targeted through social media with fake checks and supposed art or “muse” payments.[6]

Never use your bank account to move money for someone you met online. Do not deposit a check and send part back. Ask a bank employee or trusted adult before acting.

Marketplace and Gaming Scams

Scams appear in resale apps, concert-ticket groups, game-item trades, and direct messages.

Warning signs include:

- leaving the platform's protected payment system;
- paying friends-and-family for a purchase;
- gift cards or cryptocurrency;
- a seller who refuses a live verification step;
- screenshots presented as proof of payment;
- "verification" links sent by the buyer;
- a request to pay a fee before receiving money;
- urgency because "another buyer is waiting."

A screenshot can be edited. Check the transaction inside the official payment app or account.

Job, Scholarship, and Influencer Scams

Teens are attractive targets because many are applying for first jobs, scholarships, auditions, teams, and creator opportunities.

A legitimate employer does not need you to:

- buy equipment with a check they emailed;
- pay for training before an interview;
- send a Social Security number through an unverified chat;
- receive packages and reship them;
- transfer money through your account;
- download remote-control software during recruitment;
- recruit friends before you can be paid.

Research the organization independently. Look for a real domain, physical presence, established contact information, and job listing on the organization's own site. Contact the organization using information you found yourself.

AI Makes Scams More Believable

Generative AI can create polished writing, cloned voices, fabricated images, and convincing videos. Bad grammar is no longer a reliable scam detector. The FBI warns that criminals use generative AI to increase the scale and believability of fraud.[7]

Families can create an emergency verification plan:

- choose a private code word not posted online;
- ask a question only the real person would know;
- hang up and call a known number;
- contact another family member;
- do not send money until independently verified.

Do not make the code word a pet name, birthday, or fact visible online.

If You Clicked or Replied

Speed helps, but panic does not.

If You Entered a Password

- Change it immediately from the official site or app.
- If reused, change it everywhere else.
- Turn on MFA.
- Sign out other sessions.
- Review recovery details and forwarding rules.

If You Shared Financial Information

- Tell a parent or trusted adult.
- Contact the bank, card company, or payment service using an official number.
- Ask whether the payment can be stopped.
- Monitor transactions.
- Use IdentityTheft.gov when identity information is involved.

If You Installed Software or Opened an Attachment

- Disconnect from sensitive accounts.

- Update security software and run a scan.
- Tell school or work IT if the device or account belongs to them.
- Do not erase the device before asking whether evidence is needed.

If You Sent Money

Contact the payment provider immediately and report fraud. Recovery is not guaranteed, but delay reduces options. Report the account and preserve messages, receipts, usernames, and transaction identifiers.

Scenario: Jordan Verifies Outside the Message

Jordan closes the fake portal and opens the team app directly. There is no uniform alert. He calls the coach using the number already saved in his contacts. The coach confirms that several players received the same message.

The school disables a copied page, warns families, and helps one student who entered a password. Jordan's useful move was not spotting a misspelled word. It was refusing to verify a message using the message itself.

Make It Stick

MEMORY ANCHOR Pressure is the clue; verify outside the message.

Pressure Test

A polished school account says your graduation fee is overdue and your name will be removed tonight. The link uses the school colors and a padlock icon.

A. Pay quickly because the consequences are serious.

B. Reply and ask the account to prove it is real.

C. Leave the message, open the school portal yourself, and call a known school number.

BEST FIRST MOVE C. The message controls every fact inside the message. Verification must come from a channel the sender did not provide.

60-Second Drill

Save official contact routes for your school, bank or payment provider, and main email service. Then practice opening each from your home screen or a bookmark instead of a message link.

Say It Out Loud

I received an urgent request from your name. I am checking through a separate channel before I do anything.

Close the Book: Recall

Before reading the summary, cover the page and answer from memory:

1. What emotions do scams commonly use?
2. Why does a padlock icon not prove honesty?
3. What should you do with a verification code someone requests?

Chapter 5 Summary

- Scams use emotional stories to create fast action.
- Pause, leave the message, and verify through a known channel.
- A professional appearance, padlock icon, familiar logo, or correct grammar does not prove legitimacy.
- Verification codes, payment screenshots, and emailed checks can be tools of fraud.
- Never move money through your account for an online contact.
- AI can improve scam writing, voices, images, and impersonation.
- After a mistake, act quickly through official accounts and providers.

Chapter 5 Safety Checklist

☐ I can identify the emotion and deadline in a suspicious message.

☐ I verify through an app, bookmark, phone number, or person I already know.

☐ I never send login or verification codes.

☐ I check payments inside the official app, not through screenshots.

☐ I do not deposit checks and return part of the money.

- ☐ My family or close circle has an emergency verification method.
- ☐ I know how to contact my bank or payment provider quickly.
- ☐ I report phishing texts, emails, accounts, and fraudulent transactions.

Chapter 5 Discussion Questions

1. Which emotions make people most likely to act before verifying?
2. Why is correct grammar no longer a good test for scams?
3. What is the safest way to verify an urgent message from a friend?
4. Why can a deposited check appear successful before being reversed?
5. What should a school do after several students receive the same phishing message?

CHAPTER 6

AI-Generated Content, Deepfakes, and Misinformation

> ***QUICK RECALL - Do not look back:*** *How do you verify an urgent message?*
> ***Check:*** *Leave the message and use a channel you already trust.*

Maya sees a video of a local teacher insulting students during what appears to be a livestream. The teacher's face, voice, classroom, and mannerisms look right. The clip spreads through group chats before first period. Students begin demanding that the teacher be fired.

Maya notices that no one can find the original livestream. Every post traces back to the same twelve-second clip.

"Looks Real" Is No Longer a Final Answer

Artificial intelligence can generate or alter text, images, audio, and video. Some results are obvious. Others are convincing enough to create doubt, embarrassment, panic, or false certainty.

NIST identifies risks from generative AI including false or misleading content, impersonation, privacy exposure, fraud, and the use of synthetic media in disinformation.[7] The FTC has warned that voice cloning can make family-emergency and impersonation scams more believable.[8]

The correct response is not to assume everything is fake. It is to separate **content** from **verification**.

A video may look convincing and still lack a trustworthy source. A real photo may be paired with a false caption. An accurate statement may

be delivered by a fake account. An AI-generated image may illustrate a real event without documenting it.

The Five-Question Verification Habit

Before sharing a surprising claim, ask:

1. **Who originally published it?**
2. **What evidence is available beyond the post itself?**
3. **When and where was it recorded or created?**
4. **What do independent, credible sources say?**
5. **What emotion is pushing me to share before checking?**

UNESCO describes media and information literacy as a core set of skills for evaluating information, addressing misinformation, and navigating AI-shaped media environments.[9]

Trace the Claim, Not the Crowd

A thousand reposts can still come from one unsupported source. Search for:

- the earliest version you can find;
- a full-length clip instead of an excerpt;
- an official statement;
- local reporting with named witnesses;
- original documents, schedules, records, or datasets;
- multiple sources that did not simply copy one another.

Do not count five sites repeating the same anonymous post as five confirmations.

Lateral Reading

Lateral reading means leaving the page to investigate the source. Instead of studying a suspicious site only from inside the site, open new tabs and search for:

- who owns or funds it;

- whether experts recognize it;
- whether it has a history of corrections;
- whether the author exists and has relevant expertise;
- whether the domain imitates a known organization;
- what independent sources say about the claim.

Professional design is cheap. Reputation must be checked elsewhere.

Image and Video Checks

No single “AI detector” can provide perfect certainty. Detection tools can make mistakes, especially after compression, editing, screenshots, or new generation methods. Use a combination of evidence.

Search the Image

A reverse-image search may reveal an older use, different caption, stock source, or original creator. Crop to the important area and try more than one search engine.

Examine Context

Look for consistent weather, shadows, reflections, signs, uniforms, architecture, language, and event details. Visual errors can be clues, but AI quality improves quickly. Do not rely only on strange hands or blinking.

Find the Full Clip

Short clips remove context. Search key phrases, usernames, visible logos, or spoken lines. Check whether the original account actually posted it.

Listen for the Ask

In scams, the most important clue may not be whether a voice is synthetic. It may be the demand: secrecy, money, a code, a transfer, or immediate action. Verify the situation through another channel.

Check Provenance Carefully

Some tools attach content credentials, signatures, or labels showing how media was created or edited. These can help, but absence of a label does not prove that content is real, and labels may be removed by screenshots or platform processing. NIST continues to study provenance, watermarking, detection, and authentication methods for synthetic content.[7]

AI Hallucinations and Confident Errors

Generative AI systems can produce false statements, invented sources, inaccurate summaries, or fabricated quotations in a confident tone. This is sometimes called hallucination.

Use AI as a starting tool, not an unquestioned authority. For schoolwork, health, law, money, safety, and current events:

- ask for sources;
- open the sources yourself;
- verify that the source says what the answer claims;
- check dates;
- distinguish a primary source from a summary;
- do not submit invented citations;
- follow school rules on AI assistance and disclosure.

Never paste highly sensitive information into an AI tool unless you understand how the service uses, stores, and shares data. Avoid uploading private medical records, intimate images, identification documents, school discipline records, confidential work files, or another person's private messages.

Manipulated Intimate Images

AI can be used to create fake sexual images or videos of a real person. The fact that an image is fake does not make the harm fake. Creating, threatening to share, or distributing such material may violate platform rules and laws. The 2025 TAKE IT DOWN Act covers certain nonconsensual intimate "digital forgeries," and as of May 19, 2026,

covered platforms must provide a notice-and-removal process and remove qualifying material and known identical copies within forty-eight hours of a valid request.[13]

Do not forward the image to prove it exists. Preserve safer evidence such as URLs, usernames, dates, report numbers, and screenshots that avoid unnecessary redistribution. Seek adult and professional help.

The Difference Between Misinformation and Disinformation

- **Misinformation** is false or misleading information shared without necessarily intending harm.
- **Disinformation** is false or misleading information created or spread deliberately to deceive.
- **Malinformation** is genuine information used out of context or shared to cause harm, such as publishing a private address.

Your response does not need to depend on knowing the creator's motive. Slow the spread, correct the record with reliable evidence, and avoid humiliating people who were fooled. Shame can make someone defend a false claim more strongly.

Scenario: Maya Finds the Source Gap

Maya searches the teacher's name and the quoted phrase. No full video appears. She checks the school's official account and local news. A longer clip later surfaces: a student created a face-and-voice replacement as a joke, then someone removed the label and reposted it as real.

Maya does not attack the students who believed it. She posts the verified school statement, links the full explanation, and asks group-chat members to stop circulating the clip.

The best correction is not "You are stupid." It is "Here is the original context, here is the evidence, and here is what we should stop sharing."

Make It Stick

MEMORY ANCHOR Trace before you share.

Pressure Test

A twelve-second clip appears to show a student threatening someone. Everyone in the group chat is reposting it, but no one has the original account or full video.

A. Share it with a warning so people stay safe.

B. Wait for a trustworthy original source, full context, and independent confirmation.

C. Use one AI detector and treat its result as final.

BEST FIRST MOVE B. Urgency does not make unsupported content safe to amplify. A detector is one clue, not a verdict.

60-Second Drill

Choose one surprising claim from your feed. Open three tabs: the original source, an independent source, and a search for earlier versions or context. Write one sentence explaining what is verified, what is uncertain, and what would change your conclusion.

Say It Out Loud

I cannot find the original or independent confirmation, so I am not forwarding this yet.

Close the Book: Recall

Before reading the summary, cover the page and answer from memory:

1. What is lateral reading?
2. Why are five copied articles not five independent sources?
3. How can a real photo carry a false claim?

Chapter 6 Summary

- Convincing media still requires source verification.

- Trace a claim to its original source and look for independent evidence.
- Use lateral reading instead of trusting a site's appearance or self-description.
- Reverse-image search, full-context search, provenance, and independent reporting work better together than any single detector.
- AI systems can produce confident errors and invented citations.
- Fake intimate images can cause real harm and may qualify for removal and reporting processes.
- Correct misinformation with evidence rather than humiliation.

Chapter 6 Safety Checklist

- ☐ Find the original source before sharing a shocking clip.
- ☐ Search outside the page to evaluate the publisher.
- ☐ Check date, location, full context, and independent reporting.
- ☐ Use reverse-image search for suspicious photos or profiles.
- ☐ Treat AI-generated answers as claims to verify.
- ☐ Do not upload sensitive personal data to AI tools without understanding the risk.
- ☐ Do not forward manipulated intimate content.
- ☐ Save URLs, usernames, dates, and report confirmations when documenting abuse.

Chapter 6 Discussion Questions

1. Why can a real photo still support a false claim?
2. What makes multiple sources truly independent?
3. Why should AI detectors not be treated as final proof?
4. How can a correction reduce harm without humiliating people?
5. What kinds of information should never be pasted into a public AI tool?

CHAPTER 7

Online Friendships, Romance, and Grooming

> ***QUICK RECALL - Do not look back:*** *What must convincing media still have?*
> ***Check:*** *A traceable source and independent evidence.*

Fourteen-year-old Nia meets “Alex” in a music fan server. Alex remembers her favorite bands, checks in after bad school days, and says she is more mature than most people her age. After two weeks, Alex asks to move to an encrypted app because “people in the server are fake.”

Then the requests change. Alex wants Nia to keep their friendship secret, stay awake for late calls, and prove she trusts him by sharing private photos.

None of the early messages looked threatening. That is why the pattern matters.

Online Relationships Can Be Real

Friendships formed online can be meaningful, supportive, and lasting. People find communities around disability, identity, hobbies, rare interests, grief, art, gaming, and experiences that may be difficult to discuss locally.

Safety guidance should not pretend those relationships are fake. It should help you judge behavior rather than rely on a profile, age claim, follower count, mutual friend, or shared interest.

A person can be exactly who they say they are and still be manipulative. A person can also use a real-looking history, stolen photos, compromised account, or AI-generated identity.

Grooming Is a Process

NCMEC defines online enticement as communication with a person believed to be a child for the purpose of sexual offenses or abduction, and notes that grooming can include sextortion, sexual conversation, image requests, or attempts to meet.[10]

Grooming often develops through stages that may overlap:

1. **Access:** finding a young person through social media, gaming, livestreams, comments, or mutual groups.
2. **Selection:** noticing loneliness, conflict, insecurity, money problems, identity questions, or a desire for attention.
3. **Trust:** offering praise, gifts, advice, protection, opportunity, or intense understanding.
4. **Isolation:** moving to private channels, criticizing friends or family, and demanding secrecy.
5. **Desensitization:** introducing sexual jokes, questions, images, or boundary tests gradually.
6. **Control:** using guilt, threats, money, private information, or images to force continued contact.

Not every friendly adult is grooming. Not every age-gap conversation is exploitative. Look for the combination of secrecy, escalating boundaries, sexualization, isolation, and control.

Red Flags That Matter More Than Profile Details

Be cautious when someone:

- refuses reasonable verification but demands yours;
- becomes intensely attached almost immediately;
- says you are “mature for your age” to justify adult behavior;
- asks you to hide the relationship from trusted people;
- sends sexual content without consent;
- asks about sexual experience early;

- offers money, gifts, game items, modeling, or career help tied to private contact;
- pressures you to move to disappearing or encrypted messages;
- gets angry when you do not reply quickly;
- threatens self-harm if you leave;
- says your family or friends are jealous and cannot understand;
- requests photos with specific clothing, poses, or surroundings;
- turns ordinary images into sexual comments;
- asks to meet secretly or arrange transportation;
- keeps returning through new accounts after being blocked.

Healthy people respect a slower pace and a no.

Verify Without Taking Dangerous Risks

Verification reduces some risks but does not create trust by itself.

Useful steps include:

- reverse-image searching profile photos;
- checking whether the account has a believable history rather than a burst of recent posts;
- requesting a live video conversation that includes a spontaneous action;
- noticing contradictions in age, school, time zone, or life details;
- telling a trusted person about the relationship;
- keeping early conversations on platforms with reporting tools;
- refusing to provide identification, address, school schedule, or live location.

A live video can also be faked or manipulated. More importantly, a verified identity does not guarantee safe intentions.

Meeting Someone From Online

The safest choice for a minor is to involve a parent or trusted adult. If a meeting is appropriate:

- meet in a busy public place during daytime;

- use your own transportation and return plan;
- bring a trusted person;
- share the plan and live location with someone safe;
- do not change locations unexpectedly;
- keep food and drinks under your control;
- leave if the person pressures you, arrives with unexpected people, or is not who they claimed;
- do not enter a private home, hotel, or vehicle.

A person who cares about your safety will not be offended by precautions.

Online Romance and Financial Manipulation

Romance scams are not limited to older adults. A person may build daily intimacy, then ask for money, gift cards, cryptocurrency, account access, or help with an emergency. FTC guidance recommends never sending money or gifts to an online romantic interest you have not met and independently verified, and suggests reverse-image searches and talking to someone you trust when concerns appear.[6]

Teen-specific versions may involve:

- game currency;
- concert tickets;
- phone bills;
- travel money;
- “borrowing” a payment account;
- buying private content;
- investment tips;
- receiving packages;
- sharing streaming or shopping logins.

Emotional closeness does not make a financial request safe.

Secrecy Versus Privacy

Privacy says, “This relationship is personal.” Dangerous secrecy says, “No trusted person can know because they would stop me.”

Ask yourself:

- Would this person continue the relationship if a trusted adult knew?
- Do I feel free to say no?
- Am I becoming more connected to my real life or more isolated from it?
- Do they support my sleep, school, friendships, and boundaries?
- Do they keep changing the rules of what I must prove?
- Am I afraid of what happens if I leave?

Fear is important information.

If You Are Already Involved

You do not need to prove that a person is a predator before seeking help. You can show a trusted adult the messages and say, “I am not sure what this is, but I feel pressured.”

If the person knows your address, school, schedule, or family information, do not announce your plan to expose them. Save evidence and make a safety plan. Block and report when it is safe to do so. Contact NCMEC’s CyberTipline when a minor is being sexually exploited or enticed.[19]

Do not meet them to “catch” them. Do not ask friends to threaten them. Do not continue sexual conversations to collect more evidence. That can increase danger and trauma.

Scenario: Nia Breaks the Isolation

Nia tells her older cousin, who responds without yelling. Together they save the username, profile link, dates, and message screenshots. They do not download or resend explicit material. Nia blocks Alex after the

evidence is secured. Her parent and cousin help report the account and make a CyberTipline report.

The account's photos belong to a real teenager in another state. The person messaging Nia was not that teenager.

The turning point was not a perfect technical investigation. It was breaking the secrecy.

Make It Stick

> **MEMORY ANCHOR** Real connection does not demand secrecy, proof, or fear.

Pressure Test

A new online friend is supportive, sends gifts, and says you are the only person who understands them. They ask you to hide the friendship, stay up for private calls, and send a photo to prove trust.

A. Send a harmless photo so they calm down.

B. Move to disappearing messages to protect both of you.

C. Tell a trusted person, preserve pressure or threats, refuse the proof demand, and end or report contact safely.

> **BEST FIRST MOVE** C. The problem is the pattern: intense attachment, isolation, escalating proof, and control.

60-Second Drill

List three people who know about your important online relationships. For any relationship no one knows about, ask whether that is ordinary privacy or whether fear and pressure are keeping it secret.

Say It Out Loud

I do not prove trust with secrecy, money, passwords, images, or location. Do not ask again.

Close the Book: Recall

Before reading the summary, cover the page and answer from memory:

1. Name the broad stages of grooming.
2. Why does identity verification not prove safe intentions?
3. What precautions belong in any online-to-offline meeting?

Chapter 7 Summary

- Online friendships can be genuine and still require boundaries.
- Grooming is usually a gradual process involving access, trust, isolation, sexualization, and control.
- Behavior matters more than a convincing profile.
- Verification lowers uncertainty but does not prove good intentions.
- Safe in-person meetings require adult involvement, public settings, independent transportation, and a clear exit.
- Secrecy, escalating proof, and fear are major warning signs.
- Do not investigate a suspected exploiter alone; preserve evidence and involve trusted adults and reporting services.

Chapter 7 Safety Checklist

☐ At least one trusted person knows about important online relationships.

☐ I do not share live location, address, school schedule, or identification with new contacts.

☐ I stay on reportable platforms during early conversations.

☐ I recognize secrecy, isolation, gifts, sexual escalation, and guilt as possible grooming tactics.

☐ I do not send money or account access to an online romantic interest.

☐ Any in-person meeting includes a trusted adult and a public safety plan.

☐ I will not meet or confront someone to collect evidence.

☐ I know how to reach the NCMEC CyberTipline.

Chapter 7 Discussion Questions

1. Why can grooming feel like support at the beginning?
2. What is the difference between privacy and isolation?

3. Which verification methods can be faked, and what can they still tell you?
4. Why might a manipulator give gifts before making demands?
5. What response from an adult would make a teenager more likely to disclose pressure early?

CHAPTER 8

Sextortion and Image-Based Abuse—Stop, Save, Tell, Report

> ***QUICK RECALL - Do not look back:*** *What three relationship signals matter more than a polished profile?* ***Check:*** *Secrecy, escalating proof, and fear or control.*

Jordan receives a follow request from someone who appears to be another teenager. They message for an hour, trade ordinary selfies, and begin flirting. The person sends a sexual image and asks Jordan to send one back. He does.

Seconds later, the conversation changes. The person sends screenshots of Jordan's followers, school team, and family accounts. "Pay $500 now," the message says, "or everyone gets it." A countdown begins.

Jordan feels as if his entire life has collapsed into one screen.

First: This Is a Crime, Not a Private Failure

Sextortion occurs when someone threatens to release private or sexual material to demand money, more images, sexual activity, or another action. The FBI has reported a major increase in cases involving children and teens and emphasizes that victims should come forward rather than continue complying.[11]

> This is not rare, and you are not the only person who has felt trapped by it. NCMEC reported receiving more than 50,000 reports of financially motivated sextortion in 2025 - an average of 137 reports per day. That number does not make the harm ordinary; it proves that specialized helpers know this pattern and that silence protects the offender, not the victim.[30]

Image-based abuse includes creating, sharing, or threatening to share intimate images without consent. The image may be real, altered, or AI-generated.[26]

The most important message is simple:

Sending an image does not give someone the right to threaten, distribute, or control you.

You may regret a choice. The offender chose the crime.

The Emergency Response: Stop, Save, Tell, Report

Panic makes every demand feel immediate. Use four words as a script.

1. Stop

- Stop replying.
- Do not send more images.
- Do not pay.
- Do not negotiate.
- Do not threaten the offender.
- Do not meet them.

Paying rarely creates control. It can confirm that you are frightened and able to send money, which may lead to more demands. Sending another image gives the offender more material.

2. Save

Before blocking or deleting the account, preserve useful evidence:

- username and display name;
- profile URL;
- platform name;
- dates and times;
- threats and payment demands;
- requested payment method, account, wallet address, or gift-card information;

- phone numbers, email addresses, and linked accounts;
- report confirmation numbers;
- screenshots showing the threat and context.

Avoid creating additional copies of illegal or intimate material. Do not forward it to friends, post it publicly, or ask others to save it. A trusted adult or law-enforcement professional can advise how to preserve necessary evidence safely.

3. Tell

Tell a parent, caregiver, counselor, teacher, coach, school safety official, or another trusted adult. Use direct words:

> *"Someone is threatening to share a private image of me. I need help saving evidence and reporting it. Please do not take my phone or contact them until we make a plan."*

If the first adult reacts badly, tell another. A poor first response does not mean help is unavailable.

4. Report

For a minor in the United States:

- report suspected child sexual exploitation to NCMEC's CyberTipline;[19]
- report the account and messages to the platform;
- contact local law enforcement or the FBI when appropriate;
- file an IC3 complaint for internet-enabled extortion or fraud;[18]
- use Take It Down if an intimate image or video taken when you were under eighteen may be online.[12]

If you are in immediate danger, call 911. If the threat has caused suicidal thoughts, self-harm urges, or an emotional crisis, call or text 988 and stay with a safe person.[17]

Take It Down: Hashing Without Uploading the Image

NCMEC's Take It Down service can help prevent or limit the spread of nude, partially nude, or sexually explicit images or videos taken when a person was under eighteen. It creates a digital fingerprint, called a hash, on the user's device. The image itself does not leave the device and is not viewed by NCMEC. Participating platforms can compare content against the hash and take action.[12]

Important limitation: Take It Down works only where participating companies scan public or unencrypted services. It does not guarantee removal from encrypted chats, private devices, nonparticipating sites, foreign hosts, or every copied file. Continue using platform reports, the CyberTipline, and local professional help as appropriate.

Important limits:

- It does not search the entire internet.
- It works only with participating services and accessible copies.
- It does not replace reporting threats or exploitation.
- You should not download an image from somewhere else in order to use the tool.
- Use the original file already on your device when available.

Take It Down can be used from anywhere in the world by a person who was under eighteen in the image, according to NCMEC's current guidance.[12]

The TAKE IT DOWN Act and Platform Removal

The federal TAKE IT DOWN Act covers certain nonconsensual intimate images, including qualifying digital forgeries and AI-generated deepfakes. Covered platforms must offer a clear notice-and-removal process. As of May 19, 2026, the FTC states that platforms must remove qualifying images and known identical copies within forty-eight hours of a valid request. If a covered platform fails to comply, it can be reported to the FTC at its dedicated portal.[13]

The law is a tool, not a reason to handle the crisis alone. A trusted adult, victim advocate, school official, or attorney may help with the process. Laws also vary by state and country.

What Adults Should Do in the First Hour

A calm adult can prevent a second crisis.

Say

- "I am glad you told me."
- "You are not in trouble for asking for help."
- "We will not pay or send more."
- "We will save evidence before blocking."
- "This threat is the offender's responsibility."

Do Not

- interrogate the teen about every decision;
- contact the offender in anger;
- post warnings that reveal the victim's identity;
- forward the image to prove what happened;
- immediately reset or destroy the device before preserving evidence;
- threaten permanent loss of all technology;
- promise that no one else will ever need to know.

Adults should explain each next step and preserve the teen's voice wherever safety permits.

When the Offender Says They Already Sent It

The offender may claim the image was sent even when it was not. They may show fake screenshots, scheduled messages, or edited recipient lists. Do not let that claim force payment.

If distribution occurred:

1. Continue preserving evidence.
2. Report every post or message through the platform's intimate-image or child-safety channel.

3. Ask recipients not to open, save, forward, comment on, or retaliate with the content.
4. Involve school administration if students or school systems are involved.
5. Use Take It Down and platform removal tools.
6. Report threats and exploitation to NCMEC and law enforcement.
7. Seek emotional support; distribution can feel devastating even when removal begins quickly.

The goal is containment, not public argument.

Supporting a Friend

A friend may tell you first because they fear an adult reaction. You can help without carrying the entire crisis.

Say:

- “I believe you.”
- “Do not pay or send more.”
- “Let’s save the threats.”
- “We need an adult who can help us report this.”
- “I will stay with you while we tell them.”

Do not:

- ask to see the intimate image;
- forward or store it;
- pose as the victim to threaten the offender;
- collect money;
- promise absolute secrecy;
- handle suicide threats alone.

If your friend says they may harm themselves, stay connected, contact 988 or emergency services, and tell an adult immediately—even if they asked you not to.

The Shame Trap

Offenders depend on shame. They want the victim to think:

- “My parents will hate me.”
- “I broke the law.”
- “My life is over.”
- “I have to fix this alone.”
- “Paying is the only way out.”

These thoughts are part of the trap, not proof. Thousands of families, advocates, investigators, and counselors have handled similar cases. Your situation deserves a response plan, not a verdict on your character.

Scenario: Jordan Breaks the Countdown

Jordan puts the phone face down and walks to his older sister’s room. He cannot say everything at first, so he shows her the threat. She tells him he is not in trouble and calls their parent.

They save the account details and payment demand, submit platform and CyberTipline reports, and contact local law enforcement. Jordan uses Take It Down with the original image on his device. He blocks the account after evidence is secured.

The offender creates a new account. Jordan does not respond. He adds the new username to the existing report. The demands stop after two days. The fear takes longer, so Jordan speaks with a counselor and keeps his phone outside his bedroom for several nights—not as punishment, but so he can sleep.

The countdown was designed to make him believe he had no time. Telling someone created time.

Make It Stick

MEMORY ANCHOR Stop. Save. Tell. Report. Never pay.

Pressure Test

Someone gives you ten minutes to pay before they send an image to your school contacts. They show a screenshot that appears to prove they already have the list.

A. Pay once to buy time.

B. Send another image that does not show your face.

C. Stop responding, preserve the threat and account details, tell a trusted adult immediately, and report.

> **BEST FIRST MOVE** C. Payment and additional material usually increase leverage. The countdown is designed to isolate you before help can arrive.

60-Second Drill

Without using a real harmful image, create a practice evidence note containing a fake username, profile URL, date, threat summary, payment method, and report number. Save the note where you could find it during panic.

Say It Out Loud

Someone is threatening me with an intimate image. I have stopped replying. I need safety first, not punishment. Please stay with me while we save evidence and report it.

Close the Book: Recall

Before reading the summary, cover the page and answer from memory:

1. What four actions form the emergency response?
2. Why should you avoid forwarding an image as proof?
3. What does Take It Down do on the device?

Chapter 8 Summary

- Sextortion is coercion and a crime; image-sharing regret does not make the threat your fault.
- Use the sequence: Stop, Save, Tell, Report.

- Do not pay, negotiate, meet, threaten, or send more material.
- Preserve account details and threats without redistributing intimate content.
- NCMEC's CyberTipline and Take It Down are major resources for minors.
- The TAKE IT DOWN Act creates a platform-removal process for qualifying nonconsensual intimate material, including certain AI-generated content.
- Immediate emotional safety matters as much as technical removal.

Chapter 8 Safety Checklist

- ☐ Stop responding and do not pay or send more.
- ☐ Save usernames, links, threats, dates, payment details, and report numbers.
- ☐ Tell a trusted adult immediately.
- ☐ Report the account to the platform.
- ☐ File a CyberTipline report for child sexual exploitation.
- ☐ Use Take It Down when an eligible image may be circulating.
- ☐ Contact IC3 or law enforcement for extortion and threats.
- ☐ Call or text 988 if panic becomes a mental-health crisis.

Chapter 8 Discussion Questions

1. Why does paying often increase rather than end an offender's control?
2. What evidence is useful without forwarding intimate material?
3. Which adult response is most likely to encourage early disclosure?
4. What are the limits of a hashing and takedown tool?
5. How can a friend support a victim without becoming the investigator?

SECTION

PART II CHECKPOINT

The Scholarship Account

This checkpoint mixes phishing, AI impersonation, grooming tactics, and image-based pressure.

> **RULE** Choose the safest first move, not the action that solves everything at once.

1. The Offer

A verified-looking account says you were selected for a scholarship because of your art. It gives you twenty minutes to complete a private form. What pattern should you name first?

2. The Voice Note

The account sends a voice note that sounds like your teacher. Is the voice enough to verify the offer?

3. The Move

The “coordinator” asks you to move to disappearing messages because other applicants are jealous. What changed?

4. The Proof

They request a private photo and a small “refundable identity fee.” What are the safest next actions?

5. The Friend

A friend says to keep chatting so you can collect evidence. Why is that risky?

Answer Key and Reasoning

1. Name the urgency-and-authority story. Pause before examining the polished details.

2. No. Voice cloning and compromised accounts make the voice only one clue. Verify through the school or teacher contact you already have.

3. The interaction is moving toward isolation and reduced reporting. Refuse the move and tell a trusted person.

4. Do not pay or send the image. Save the account, request, links, and messages; verify the scholarship independently; block and report after evidence is secured.

5. Continuing can increase manipulation, expose more information, and create additional harmful material. A teen should not conduct an undercover investigation.

Teach It Back

Explain the checkpoint to another person in sixty seconds. Use the memory anchors, not the chapter titles. If you cannot explain the first move without looking, review only the section you missed and try again tomorrow.

PART III

Protect Your Community

Connection grows stronger when control, judgment, and recovery skills grow with it.

CHAPTER 9

Social Media Without Losing Yourself

> ***QUICK RECALL - Do not look back:*** *What is the first rule of sextortion response?*
> ***Check:*** *Do not pay or send more. Stop, save, tell, and report.*

Maya posts a drawing she spent six hours making. It gets fourteen likes. A rushed joke posted the next day gets three thousand views. She tells herself numbers do not matter, then refreshes the analytics every few minutes.

By midnight, she is changing what she creates based on what the platform rewarded that afternoon.

Platforms Measure Attention, Not Worth

Views, likes, shares, streaks, follower counts, and watch time are measurements inside a platform. They can reveal reach or engagement. They cannot measure the quality of your friendships, the value of your work, your attractiveness, intelligence, future, or character.

The problem is not that metrics exist. The problem is that they are easy to mistake for a scoreboard of personal value.

Algorithms often optimize for attention. Content that creates anger, fear, envy, shock, or intense identification can hold attention. That does not mean the platform wants you to suffer; it means the system may reward material that keeps you watching regardless of how you feel afterward.

Curate the Feed You Actually Want

Your feed is shaped by what you pause on, replay, search, share, comment on, hide, and follow. Hate-watching still teaches the system that you watched.

Use active signals:

- unfollow or mute accounts that repeatedly harm your mood;
- choose “not interested” on content you do not want amplified;
- clear or pause watch and search history when recommendations become distorted;
- follow sources and creators that add useful, varied material;
- turn off autoplay when it traps you;
- use chronological or following feeds where available;
- disable nonessential notifications;
- reset recommendation profiles when the service permits.

Curation is not avoiding every uncomfortable idea. It is refusing to let an engagement system choose your emotional diet without input.

Private Accounts Still Need Public Judgment

A private account limits access; it does not eliminate copying. Followers can screenshot, screen-record, impersonate, or lose control of their accounts.

Before posting to a limited audience, ask:

- Do all current followers still belong here?
- Am I posting someone else’s private information?
- Does this reveal a live location or conflict?
- Would a screenshot create a safety problem?
- Am I posting while angry, intoxicated, exhausted, or panicked?
- Is this a joke that depends on hidden context?

You do not need to make every post future-employer-safe. You do need to understand the audience is never perfectly sealed.

Close Friends Lists and Secondary Accounts

“Close friends,” private stories, and secondary accounts can create more honest spaces. They can also create social pressure: Who was included? Who was removed? Why did a private joke leak?

Use them as access controls, not as guarantees. Review the list. Avoid using a private audience to organize harassment, share intimate images, or post someone’s confidential disclosure. Smaller audiences can still cause large harm.

Comparison Is an Unequal Contest

You usually see other people’s selected moments and your own unedited life. You see their finished photo and your failed attempts, their acceptance and your waiting, their vacation and your ordinary Tuesday.

Comparison becomes especially harmful when content is filtered, staged, sponsored, surgically altered, or AI-generated without clear disclosure. Notice the effect rather than arguing with yourself about whether you “should” be affected.

Try a three-part check:

1. What did I consume?
2. How do I feel afterward?
3. What action would improve the next ten minutes?

The action might be muting an account, leaving the app, texting a friend, eating, sleeping, stretching, creating something without posting it, or asking for help.

Advertising, Influencers, and Hidden Persuasion

Online ads may look like entertainment, reviews, challenges, or personal recommendations. Influencers may be paid, receive free products, use affiliate links, or have financial interests that are not obvious.

Before buying or copying advice:

- look for sponsorship disclosures;
- search independent reviews;
- compare total cost, subscriptions, and return policies;
- be skeptical of countdown timers and “secret” methods;
- distinguish personal experience from evidence;
- do not treat popularity as professional qualification;
- ask whether a body, lifestyle, or income claim depends on filters, editing, or missing context.

The FTC has repeatedly addressed blurred advertising and youth-directed marketing, including in games and creator content.[23]

Posting Through Conflict

Public conflict creates an audience, and audiences reward escalation. If a disagreement begins in private, moving it to stories or group chats can make resolution harder.

Before posting a callout:

- Is there an immediate safety reason the public needs to know?
- Have I verified the claim?
- Am I exposing a minor, address, private image, or medical information?
- Can I describe behavior without inviting harassment?
- Would a direct report to the platform, school, workplace, or law enforcement be more effective?
- Am I prepared to correct the post if new evidence appears?

Accountability and dogpiling are not the same. A call for help should not become a request for strangers to threaten someone.

Scenario: Maya Separates Creating From Posting

Maya hides public like counts where possible and creates a rule: she will not check analytics for twenty-four hours after posting art. She

starts a private folder of work that never goes online and schedules posts rather than publishing whenever she feels insecure.

Her engagement does not immediately increase. Her ability to finish a drawing does.

Make It Stick

MEMORY ANCHOR Your feed learns from what you pause on.

Pressure Test

A creator's posts leave you anxious and angry, but you keep watching every video to prove the claims are ridiculous. The platform sends you more of the same content.

A. Keep hate-watching so you understand the trend.

B. Argue in every comment section.

C. Stop rewarding the content with attention; mute, unfollow, mark not interested, and deliberately engage with what you want more of.

BEST FIRST MOVE C. Recommendation systems can treat outrage, replays, comments, and long viewing as interest.

60-Second Drill

Retrain ten signals: unfollow or mute three accounts, mark three recommendations not interested, turn off two nonessential notifications, and deliberately search for two useful or enjoyable topics.

Say It Out Loud

I do not owe this post my attention, reaction, or immediate reply.

Close the Book: Recall

Before reading the summary, cover the page and answer from memory:

1. What do platforms often optimize that is different from well-being?
2. Why can a private story still create public harm?
3. What is a safe rule for posting during conflict?

Chapter 9 Summary

- Platform metrics measure platform activity, not personal value.
- Recommendation systems learn from attention, including negative attention.
- Privacy settings reduce audience size but cannot prevent copying.
- Comparison often matches someone else's selected image against your complete life.
- Advertising and influence can be hidden inside ordinary content.
- Public conflict should be handled with evidence, proportionality, and concern for collateral harm.

Chapter 9 Safety Checklist

- ☐ Disable nonessential notifications and autoplay.
- ☐ Mute, unfollow, or mark "not interested" when content repeatedly harms my mood.
- ☐ Review close-friends and private-story audiences.
- ☐ Wait before posting while angry, exhausted, or panicked.
- ☐ Check sponsorships and independent reviews before buying.
- ☐ Keep some creative work and personal moments offline.
- ☐ Avoid posting private information during conflict.
- ☐ Correct or remove claims when evidence changes.

Chapter 9 Discussion Questions

1. What does a view count measure, and what can it never measure?
2. How does hate-watching affect recommendations?
3. When can a public callout protect people, and when can it become harassment?
4. What is gained by creating something that is never posted?
5. Which notification would you miss least if it disappeared today?

CHAPTER 10

Gaming, Livestreams, and Group Chats

> ***QUICK RECALL - Do not look back:*** *What does a private account fail to prevent?*
> ***Check:*** *Screenshots, copied content, compromised followers, and off-platform sharing.*

Eli joins a competitive game server after a teammate recommends it. The group is funny, skilled, and welcoming. Members help him improve and give him rare in-game items. After a month, a moderator asks Eli to install a “performance tool” and share his screen while logging in so the moderator can configure it.

Eli hesitates. The moderator reminds him how much the group has given him.

Games Are Social Spaces

Online games are not only games. They are voice rooms, economies, communities, performance stages, and identity spaces. The same features that support friendship and teamwork can support scams, grooming, harassment, and account theft.

NCMEC notes that gaming can support social and problem-solving skills while still carrying risks.[23] The FBI has warned that communication features in games can be used by predators and that newer violent online networks may recruit or coerce vulnerable youth through gaming and messaging spaces.[24]

The lesson is not to fear every teammate. It is to treat gaming relationships with the same boundary skills used elsewhere.

Protect the Account and the Inventory

Gaming accounts may contain payment cards, personal messages, valuable skins, rare items, saved addresses, voice recordings, and links to console or social accounts.

Use:

- a unique password or passkey;
- MFA;
- official marketplaces and trade systems;
- purchase PINs;
- login alerts;
- privacy controls for voice, text, invites, and friend requests;
- separate child or teen settings where appropriate;
- backups for recovery codes.

Do not share login credentials for boosting, ranking, item duplication, beta access, or tournament registration.

Common Gaming Scams

- fake free-currency generators;
- counterfeit tournament or clan invitations;
- login pages for item voting or trades;
- “verification” bots that request credentials;
- malware disguised as mods, cheats, launchers, or optimization tools;
- payment disputes after off-platform trades;
- account-recovery scams;
- fake support staff;
- QR codes that authorize logins;
- screen-sharing requests that expose codes, email, or recovery information.

Use official stores and known community repositories. A popular video or server endorsement is not proof that a file is safe.

Mods, Cheats, and Unknown Software

Installing a mod changes software. Some communities review code and maintain trusted repositories; others distribute executable files through temporary links.

Before installing:

- confirm the game allows it;
- use the official or established source;
- check independent community reputation;
- scan files with current security tools;
- avoid disabling antivirus because a stranger says it is a “false positive”;
- back up important saves;
- do not grant administrator access unless clearly necessary;
- never install remote-control software for a teammate.

Cheat software is a frequent cover for account stealers and malware. Even when it works, it may expose the device and violate game rules.

Voice Chat and Accidental Disclosure

Voice chat can reveal:

- your age;
- full name when someone nearby calls you;
- family conflict;
- school announcements;
- location clues;
- other people’s private conversations;
- smart-speaker responses;
- personal notifications;
- emotional vulnerability.

Use push-to-talk when practical. Mute when someone enters the room. Wear headphones. Avoid giving strangers a live tour of your home through a camera or stream.

Livestreaming Raises the Stakes

Livestreams combine public performance with real-time location, chat, donations, and emotional pressure.

Before streaming:

- remove addresses, mail, school items, schedules, medication labels, and family photos from view;
- disable notification previews;
- use a delay for higher-risk streams;
- assign trusted moderators;
- create banned-word and link filters;
- decide what personal questions you will not answer;
- separate business contact information from personal accounts;
- avoid announcing that you are alone;
- know how to end the stream immediately.

A viewer donating money does not purchase access to your body, private messages, location, or time.

Swatting, Doxxing, and Threats

Swatting is a false emergency report intended to send armed law enforcement to a person's location. It can be connected to doxxing, gaming disputes, extortion, or violent online networks. The FBI's IC3 has warned about youth-targeting networks involved in swatting, extortion, SIM swapping, account theft, and violence.[24]

If someone threatens to swat or dox you:

1. save the threat, username, links, and context;
2. do not challenge them to prove it;
3. tell a parent or trusted adult;
4. report to the platform;
5. contact local law enforcement through a non-emergency number to ask about documenting a credible threat;
6. secure accounts and remove public address clues;

7. report internet-enabled threats to IC3;
8. call 911 if danger is immediate.

Do not post the threat publicly with your address or additional personal details visible.

Group Loyalty Can Become Control

Groups build trust through shared language, jokes, ranks, gifts, and secrets. A harmful group may gradually require members to:

- prove loyalty through illegal or humiliating acts;
- harass a target;
- share explicit content;
- expose personal information;
- participate in raids or threats;
- cut off outsiders;
- livestream self-harm or violence;
- stay silent about criminal behavior.

The FBI has warned that some violent online networks use threats and blackmail to coerce minors into producing sexual, violent, or self-harm content.[24]

Leave and seek help when belonging depends on harm. Do not try to infiltrate, expose, or defeat such a group alone.

Scenario: Eli Refuses the "Tool"

Eli tells the moderator he will only use software linked through the game's official community page. The moderator becomes insulting and threatens to remove his items. Eli screenshots the messages, leaves the server, changes his game and email passwords, and reports the account.

A friend later admits that the "tool" stole browser sessions and game accounts. Eli lost access to a group. He kept control of his device and identity.

Make It Stick

> **MEMORY ANCHOR** Protect the account, the room, and the real-world location.

Pressure Test

A teammate offers a “private anti-cheat tool” and asks you to disable security software. During voice chat, another player repeats your first name, school mascot, and the sound of a nearby train.

A. Install it because a teammate vouched for it.

B. Leave voice chat but keep the download.

C. Do not install it, preserve the message, report the account or group, and review what the conversation revealed.

> **BEST FIRST MOVE** C. Trust in a teammate does not make unknown software safe, and voice chat can leak a location profile over time.

60-Second Drill

Check one gaming account for unique credentials, MFA, linked payment methods, trade protections, active sessions, voice privacy, and visible activity. Remove one unnecessary payment method or old session.

Say It Out Loud

I do not disable security or install private tools sent through chat. Use the official platform or leave me out.

Close the Book: Recall

Before reading the summary, cover the page and answer from memory:

1. Why are game inventories and skins financially valuable targets?
2. What can a background microphone reveal?
3. What should you do after a swatting threat?

Chapter 10 Summary

- Gaming accounts can hold real value and sensitive information.

- Free currency, trades, tournaments, mods, and performance tools are common scam covers.
- Voice and livestreams reveal information in real time.
- Donations and gifts do not create a right to personal access.
- Swatting and doxxing threats require evidence, adult support, platform reports, and sometimes law enforcement.
- Group belonging becomes dangerous when loyalty requires secrecy, crime, humiliation, sexual content, or harm.

Chapter 10 Safety Checklist

- ☐ Enable MFA and purchase controls on gaming accounts.
- ☐ Use official marketplaces and trade systems.
- ☐ Never share login codes or credentials with teammates or "support."
- ☐ Install mods only from allowed, established sources.
- ☐ Use push-to-talk and protect background conversations.
- ☐ Prepare the physical space and moderation tools before livestreaming.
- ☐ Save and report swatting, doxxing, extortion, or violent threats.
- ☐ Leave groups that demand harmful proof of loyalty.

Chapter 10 Discussion Questions

1. Why can a gift or rare item make manipulation more effective?
2. What information can leak through voice chat without being intentionally shared?
3. Why is disabling security software for a mod a major warning sign?
4. How should a streamer respond to a donor who demands private access?
5. What makes an online group a community, and what makes it coercive?

CHAPTER 11

Cyberbullying, Dogpiles, Doxxing, and Harassment

> ***QUICK RECALL - Do not look back:*** *What three things can voice chat reveal accidentally?* ***Check:*** *Identity clues, location clues, and routines.*

Sam makes a mistake during a school performance. Someone posts a clip with a cruel caption. By lunch, students have remixed it, created parody accounts, and flooded Sam's messages. One person sends a home address. Another says, "Relax, it is just a meme."

The harm is no longer one comment. It is repetition, audience, permanence, and fear.

Cyberbullying Is More Than Mean Speech

StopBullying.gov defines cyberbullying as bullying through digital devices and includes harmful, false, or mean content, as well as sharing private information intended to cause embarrassment or humiliation.[14]

Online harm can include:

- repeated insults or threats;
- rumor campaigns;
- impersonation accounts;
- nonconsensual image sharing;
- exclusion used as public punishment;
- mass reporting intended to silence someone;
- coordinated dogpiling;
- identity-based harassment;
- doxxing;
- stalking or monitoring;

- unwanted sexual messages;
- encouraging self-harm;
- manipulating search results or tags to connect a person with humiliating content.

A single severe threat or image can require urgent action even if it has not repeated.

Do Not Feed the Evidence Into the Harassment

When attacked, a person may want to reply to every post and prove every lie wrong. That can increase visibility and provide more content for attackers.

Use a response ladder:

1. **Assess immediate danger.** Are there threats, weapons, addresses, stalking, sexual content, or self-harm concerns?
2. **Preserve evidence.** Save dates, usernames, URLs, screenshots, and witnesses.
3. **Limit contact.** Mute, restrict, block, or filter after evidence is saved.
4. **Report through the correct category.** Threats, impersonation, intimate images, hate, and child exploitation may have separate reporting channels.
5. **Escalate offline.** Tell parents, school officials, employers, coaches, or law enforcement as appropriate.
6. **Protect mental space.** Let a trusted person monitor reports if viewing the content is harmful.

StopBullying.gov recommends not responding or forwarding, preserving evidence, and blocking and reporting the person involved. [14]

Document So Another Person Can Understand

A useful incident log includes:

- date and time;
- platform and account;

- exact behavior;
- URL or message identifier;
- screenshot file name;
- who saw it;
- report date and confirmation number;
- school or adult notified;
- any safety effect, such as missing class or changing a route.

Do not edit screenshots in ways that remove context. Keep originals and a working copy with private information redacted for sharing.

Doxxing and Personal Information

Doxxing is publishing identifying or location information to enable harassment, intimidation, or harm. It may involve a home address, phone number, family names, school, workplace, schedules, or private records.

If doxxed:

- do not repost the information while asking for help;
- save the URL and a screenshot;
- report it under privacy, harassment, or threat categories;
- tell household members and school or work security;
- remove public records and account clues where practical;
- change routines temporarily if a threat appears credible;
- consider credit freezes or identity steps if identity information was exposed;
- contact law enforcement for threats or stalking;
- search for copies after the first removal.

The fact that some information existed in a public database does not make targeted publication harmless.

Impersonation Accounts

An impersonator may post fake statements, contact friends, solicit money, distribute images, or provoke conflict.

Response steps:

1. Capture the profile, handle, URL, bio, posts, and messages.
2. Ask friends not to engage or spread it.
3. Report impersonation through the platform.
4. Post a brief notice from your real account if necessary: “This is my only account. Do not send money or information to others using my name.”
5. Secure your real account.
6. Contact school, employer, or law enforcement if threats, fraud, or sexual content are involved.

Avoid starting a public contest with the impersonator. Clear verification and reporting are more useful than escalating insults.

When School Is Involved

Cyberbullying may happen off campus and still affect school safety, attendance, learning, teams, and activities. Save evidence before asking the school to act.

A clear report states:

- what happened;
- who is involved, if known;
- how it affects school access or safety;
- what evidence exists;
- whether there are threats, sexual content, discrimination, stalking, or disability-related harassment;
- what immediate protection is requested.

Possible requests include a safety plan, schedule adjustment, no-contact directive, escort, counseling, preservation of school-system records, investigation under policy, or protection from retaliation.

School discipline and legal standards vary. Document dates and responses. If discrimination based on protected status is involved, additional civil-rights processes may apply.

Being a Bystander Without Joining the Crowd

A dogpile grows through small acts: liking, laughing, forwarding, quote-posting, or asking for the "full story." You do not have to create the attack to increase it.

Helpful bystander actions:

- do not like, share, remix, or request the content;
- report serious violations;
- message the target privately with support;
- save evidence only when needed and do not redistribute it;
- correct false claims with reliable evidence;
- tell a trusted adult when safety is involved;
- ask group admins to stop coordinated harassment;
- avoid publicly centering yourself as the rescuer.

A private "I saw what is happening. You do not deserve it. Do you want help reporting?" can matter more than a public speech.

When You Caused Harm

Maybe you posted the joke, forwarded the screenshot, or joined the comments. Accountability requires more than "sorry you were offended."

A useful repair includes:

1. Stop the behavior.
2. Delete your post and ask people you sent it to not to reshare.
3. Report copies when appropriate.
4. Apologize without excuses.
5. Name the harm you caused.
6. Ask what repair is welcome without demanding forgiveness.
7. Accept school, platform, or relationship consequences.
8. Do not turn your guilt into a request for the harmed person to comfort you.

You may not be able to erase the harm. You can stop extending it.

Scenario: Sam Builds a Case, Not a Counterattack

Sam's first screenshot shows only one insult. A counselor helps create an incident log showing two days of impersonation, address sharing, and messages encouraging self-harm. The school and platform can now see the pattern.

Sam's friend monitors the public posts so Sam does not have to keep reading them. The school makes a safety plan, the address post is removed, and the impersonation account is disabled. Some copies remain, but the dogpile loses momentum when students stop feeding it.

Make It Stick

MEMORY ANCHOR Build a case, not a counterattack.

Pressure Test

A dogpile is growing. Friends want to post the harasser's address, flood their family's accounts, and make a "proof thread" containing every cruel message.

A. Join because stronger retaliation will end it.

B. Post only the address but not the family accounts.

C. Preserve evidence privately, reduce exposure, use the right reporting path, and refuse retaliation or redistribution.

BEST FIRST MOVE C. Counter-harassment can increase danger, destroy context, expose bystanders, and make a legitimate report harder to evaluate.

60-Second Drill

Create a blank incident log with columns or lines for date/time, platform, username and URL, factual event, witness, evidence filename, report number, and safety impact. Store it somewhere accessible but private.

Say It Out Loud

I am documenting this for a report. I am not reposting private information or joining a retaliation campaign.

Close the Book: Recall

Before reading the summary, cover the page and answer from memory:

1. What makes conduct cyberbullying rather than one rude message?
2. What details make a report actionable?
3. What can a bystander do besides commenting?

Chapter 11 Summary

- Cyberbullying can include repeated harassment, impersonation, private-information exposure, image abuse, and threats.
- Save evidence before blocking or deleting.
- Use a structured incident log and the platform's specific reporting category.
- Doxxing requires privacy removal, household safety planning, and possible law-enforcement involvement.
- Bystanders can either increase or interrupt a dogpile.
- Accountability means stopping, removing, repairing, and accepting consequences.

Chapter 11 Safety Checklist

- ☐ Assess threats and immediate physical danger first.
- ☐ Save full-context evidence with dates, links, and usernames.
- ☐ Do not respond to every post or forward harmful material.
- ☐ Block, mute, restrict, and filter after evidence is preserved.
- ☐ Report impersonation, doxxing, threats, hate, or intimate images under the correct category.
- ☐ Tell school or work how the conduct affects safety and access.
- ☐ Ask a trusted person to monitor content if repeated viewing is harmful.
- ☐ As a bystander, do not like, share, remix, or request abusive content.

Chapter 11 Discussion Questions

1. When can one online act be serious even without repetition?
2. Why is an incident log more useful than a folder of unlabeled screenshots?
3. How can public defense accidentally increase a dogpile?
4. What does a meaningful apology require after digital harm?
5. Which school protections could help a student continue attending safely?

CHAPTER 12

Digital Footprints, School, Work, and Reputation

> ***QUICK RECALL - Do not look back:*** *What should you build instead of launching a counterattack?* ***Check:*** *A clear evidence record that another person can understand.*

A digital footprint is the record created by your online activity. Some parts are obvious: posts, comments, usernames, livestreams, reviews, and public profiles. Other parts are quieter: search history, device identifiers, location records, advertising profiles, account logs, and information other people post about you.

Your footprint is not a permanent moral score. People grow. Context matters. Old posts can be misunderstood, copied, or resurfaced, but one embarrassing moment does not define your future. The useful goal is not to become invisible. It is to make your public record more accurate, intentional, and difficult to misuse.

The Three Layers of a Digital Footprint

Think about your online presence in three layers.

The public layer includes anything a stranger can find without being accepted as a follower: public posts, profile photos, bios, gaming handles, public playlists, school-team rosters, comments, petitions, and tagged content.

The shared layer includes content visible to friends, followers, classmates, teams, servers, or group chats. It feels private because the audience is limited, but anyone in that audience may copy it.

The system layer includes information held by platforms and service providers: login history, purchases, message metadata, advertising interests, reports, and device data. You may not see all of it, but it can

still affect recommendations, security decisions, and what ads or content you receive.

Private browsing changes what is stored locally in that browser session. It does not make you anonymous to websites, your school or employer network, your internet provider, or other systems that can observe traffic. A virtual private network can reduce some exposure on a local network and change the apparent network location, but it does not make unsafe behavior safe or prevent an account provider from recognizing you.

Scenario: Eli Applies for a Summer Job

Eli applies to work at a community pool. He searches his name and finds an old public account with an offensive joke a friend posted from his phone when they were thirteen. The account has Eli's photo and name, so a stranger would assume he wrote it.

Eli does not panic or invent a complicated excuse. He deletes the post, changes the old account's password, enables multifactor authentication, removes unnecessary personal details, and checks whether copies appear elsewhere. He also updates his current public profile to show recent volunteer work and swim-team experience.

When the hiring manager asks about the old account, Eli answers directly: "That post was made from my phone years ago. It was wrong, and I should have secured the account and removed it sooner. I have done that." His response demonstrates judgment rather than pretending the internet never happened.

Search Yourself With a Purpose

A periodic self-search is a security check, not an invitation to obsess over every result.

Try:

- your full name in quotation marks;
- common versions of your name;
- usernames you have used;

- your name plus school, town, team, employer, or activity;
- a reverse-image search of public profile photos;
- searches while signed out, so personalization changes less of what you see.

Record results that expose private information, impersonate you, contain threats, or show content you want to address. Use platform removal tools when content violates policy. Ask the person who posted ordinary unwanted content to remove it when doing so is safe. Search engines may sometimes remove certain sensitive personal information from results even when the original page remains online, but the rules vary.

Do not pay a reputation company simply because it promises to "erase the internet." Some services are legitimate; others exaggerate their abilities or charge for steps you can take yourself. Understand exactly what will be removed, from where, for how long, and whether the source page remains available.

What Schools and Employers May See

Admissions offices, coaches, scholarship committees, employers, customers, and coworkers may see public information. They may also receive screenshots from other people. What they are permitted to consider depends on local law and institutional policy, but you should assume that clearly public material can travel beyond its original audience.

That does not mean you must become bland. Creativity, humor, advocacy, and strong opinions can be part of a healthy public identity. The question is whether your post communicates what you intend when separated from your tone of voice, friends, and original moment.

Before posting publicly, ask:

1. Who is the likely audience today?
2. Who could become the audience later?
3. Does the post expose someone else's private information?

4. Would a reasonable person understand the context?
5. Am I posting while angry, pressured, exhausted, or impaired?
6. Is this an argument that needs an audience?
7. Would I stand behind the wording if it appeared without the rest of the thread?

Build a Positive, Accurate Footprint

“Positive” does not mean fake perfection. It means giving people truthful evidence of who you are now.

You might maintain a small portfolio, publish artwork, document a project, list volunteer work, share game development, contribute to open-source software, write reviews, post athletic highlights with appropriate consent, or create a professional email address for applications. A consistent name and a short accurate bio can help people distinguish you from someone with a similar name.

Separate accounts can help keep audiences clear, but separation is not guaranteed. Reused profile photos, usernames, phone numbers, mutual contacts, and writing patterns can connect accounts. Do not use a “private” account as permission to harm people.

Cleaning Up Without Erasing Your History

Use a staged cleanup:

Secure. Change weak or reused passwords, turn on MFA, remove unknown sessions, and update recovery information.

Reduce. Remove addresses, phone numbers, routine locations, old school details, and unnecessary public birth-date information.

Review. Look through old posts, likes, public comments, tagged photos, and connected apps.

Correct. Remove false information, report impersonation, and ask for corrections where appropriate.

Rebuild. Add current work, interests, and contact information you are comfortable sharing.

Maintain. Repeat the review every few months or before a major application.

Deleting an account may not remove screenshots, quoted posts, archived pages, or records another service must retain. Still, reduction matters. Safety is often about making abuse harder, slower, and less rewarding—not proving that no copy exists anywhere.

When Someone Uses Your Past Against You

A person may threaten to expose an old post, private message, photo, or mistake to control you. That can be blackmail, coercion, harassment, or abuse depending on the circumstances.

Do not negotiate under panic. Save the threat. Tell a trusted adult. Secure your accounts. Decide whether the underlying content needs removal, explanation, or no response. Report threats through the relevant platform and, when there is extortion, stalking, sexual exploitation, or credible danger, to the appropriate authorities.

A mistake becoming public may feel catastrophic. It is usually more survivable than ongoing control by someone who benefits from your fear.

Scenario: Maya Refuses the Reputation Trap

A former friend tells Maya, “Do what I say or I’ll send everyone screenshots of what you said during our fight.” Maya is ashamed of the messages, but she notices the demand keeps changing.

She saves the threats, tells her older cousin and school counselor, changes account passwords, and writes a short factual apology to the person she insulted. She does not pay or obey the former friend. The screenshots still circulate among a few students, but the coercion ends because Maya stops treating secrecy as the price of safety.

Make It Stick

MEMORY ANCHOR Your footprint is editable, not hopeless.

Pressure Test

Someone sends an old screenshot from middle school and says they will send it to an employer unless you do what they want.

A. Comply so the screenshot stays private.

B. Delete every account immediately and hope it disappears.

C. Save the threat, tell a trusted person, report extortion or harassment, and prepare truthful context if the old post is raised.

> **BEST FIRST MOVE** C. A past mistake does not create permanent control for another person. Evidence, context, accountability, and current behavior matter.

60-Second Drill

Search your name, usernames, and profile photos while logged out. Classify the first page of results: accurate and positive, accurate but private, outdated, false, or harmful. Take one cleanup or improvement action.

Say It Out Loud

That old post does not give you control over me. I saved this threat and I am getting help.

Close the Book: Recall

Before reading the summary, cover the page and answer from memory:

1. What are the three layers of a digital footprint?
2. What can you do when deletion is impossible?
3. How can a positive footprint be built without becoming fake?

Chapter 12 Summary

- A digital footprint includes public content, limited-audience content, and data held by systems.
- Privacy tools reduce specific kinds of exposure; they do not create total anonymity.
- Search yourself periodically to find impersonation, exposed information, and outdated public content.

- A useful online reputation is accurate and current, not artificially perfect.
- Secure, reduce, review, correct, rebuild, and maintain.
- Threats to expose past content should be treated as coercion, not as proof that you must comply.

Chapter 12 Safety Checklist

- ☐ Search your name and major usernames while signed out.
- ☐ Review public bios, photos, tags, comments, and connected apps.
- ☐ Remove unnecessary school, routine, address, phone, and birth-date details.
- ☐ Secure old accounts before deleting or abandoning them.
- ☐ Report impersonation and sensitive-information exposure.
- ☐ Create a truthful public profile or portfolio when useful.
- ☐ Save threats involving blackmail, exposure, or coercion.
- ☐ Repeat the review before applications, competitions, or public events.

Chapter 12 Discussion Questions

1. Which parts of a digital footprint can you control directly, indirectly, or not at all?
2. How is an accurate online identity different from a perfect-looking one?
3. What can private browsing and a VPN do, and what can they not do?
4. When should an old post be deleted, explained, corrected, or left alone?
5. Why can accepting embarrassment be safer than obeying a blackmailer?

SECTION

PART III CHECKPOINT

The Clip in the Group Chat

This checkpoint combines social-media pressure, gaming communities, harassment, misinformation, and reputation.

> **RULE** Choose the safest first move, not the action that solves everything at once.

1. The Clip

A clip from a gaming stream appears to show a classmate using a slur. You cannot find the full stream. What do you do before reacting?

2. The Dogpile

Students begin tagging the classmate's employer and family. What is a useful bystander action?

3. The Address

Someone posts an address and says, "Go ask them yourself." What changes about the response?

4. The Old Post

Another student adds a real but unrelated post from three years ago. What kind of information problem can real material create?

5. Your Role

You reposted the first clip before checking. What does an accountable correction include?

Answer Key and Reasoning

1. Trace the original, locate full context, and seek independent confirmation. Do not treat virality as evidence.

2. Do not add comments or screenshots. Save the source privately, report coordinated harassment, tell a school or platform contact, and ask peers to stop redistribution.

3. It is now doxxing with a potential physical-safety risk. Preserve the URL and threat, involve adults or authorities, and avoid public confrontation.

4. Malinformation: genuine information can be used out of context to cause harm.

5. Remove what you control, state what was unverified, link the reliable correction, ask recipients not to reshare, and do not make the apology about your embarrassment.

Teach It Back

Explain the checkpoint to another person in sixty seconds. Use the memory anchors, not the chapter titles. If you cannot explain the first move without looking, review only the section you missed and try again tomorrow.

PART IV

Recovery, Well-Being, and Real-World Help

Connection grows stronger when control, judgment, and recovery skills grow with it.

CHAPTER 13

Mental Health, Attention, Sleep, and Algorithmic Pressure

> ***QUICK RECALL - Do not look back:*** *What is the goal of reputation cleanup?*
> ***Check:*** *Reduce inaccurate or harmful exposure while building an honest positive footprint.*

The internet can help you find friends, learn skills, organize around issues, create art, explore identity, and feel less alone. It can also become a source of comparison, conflict, sleep loss, compulsive checking, disturbing content, or pressure to perform.

Those truths can exist together. A useful conversation about mental health does not begin with “phones are evil” or “online life is not real.” It begins with a practical question: **What is this technology doing in your life right now?**

The U.S. Surgeon General has warned that we do not yet have enough evidence to conclude that social media is sufficiently safe for children and adolescents, while also recognizing that benefits and harms vary by person, platform, content, and pattern of use.[15] Current health guidance emphasizes protecting sleep, reducing exposure to harmful content, strengthening media literacy, and creating boundaries that preserve relationships and development.[15][16]

Algorithms Are Designed to Keep Choosing

A recommendation system predicts what might hold your attention. It learns from pauses, rewatches, searches, shares, comments, follows, and skips. It may show more of what produces a strong reaction—even when that reaction is fear, anger, disgust, envy, or shock.

This does not mean an algorithm controls your mind. It means the environment is not neutral. Endless feeds remove natural stopping points. Notifications create unfinished business. Streaks turn absence into a social penalty. Public metrics make approval visible. Personalized content can make a narrow belief or body ideal seem universal.

Understanding the design gives you options. You can interrupt a system without abandoning every benefit it provides.

Scenario: Nia's Feed Becomes a Mirror That Lies

Nia follows fitness creators for volleyball training. She pauses on a few dramatic "before and after" videos. Within a week, her feed is full of restrictive diets, body checking, and claims that one normal meal will "ruin progress."

Nothing on the screen explicitly orders Nia to hate her body. The repetition does the work. She begins skipping breakfast and comparing every photo of herself to edited images.

A teammate notices she seems tired. Nia unfollows several accounts, marks harmful recommendations as unwanted, clears search history where the app allows it, and follows licensed sports-dietitian and recovery-oriented sources. She talks to a parent and school nurse rather than trying to solve nutrition through a feed optimized for attention.

The algorithm did not diagnose Nia, and changing the feed is not treatment. It was one part of reducing pressure while she got real help.

Signs Your Online Pattern Needs Attention

A pattern may need adjustment when:

- sleep regularly loses to scrolling, gaming, or messaging;
- you feel unable to stop even when you want to;
- school, work, sports, hygiene, meals, or relationships are being neglected;
- you repeatedly seek content that leaves you distressed;

- notifications produce panic or constant checking;
- you judge your body, success, or relationships mainly through online comparison;
- you feel watched, evaluated, or required to respond at all hours;
- conflict online is carrying into threats, self-harm thoughts, or fear of attending school;
- taking a short break causes intense distress that feels impossible to manage alone.

These signs are information, not a character verdict. “Use more willpower” is often less useful than changing the environment, getting support, and treating any underlying anxiety, depression, trauma, attention difficulty, or sleep problem with qualified help.

Protect Sleep First

Sleep affects attention, memory, mood, learning, physical health, and impulse control. Online conflict also feels harder to solve at 2:00 a.m.

Practical changes include:

- charge the phone outside reach or outside the bedroom;
- use a real alarm clock if the phone becomes the reason it stays nearby;
- schedule Do Not Disturb, allowing calls from selected emergency contacts;
- turn off nonessential notifications;
- set a “last call” time for games and group chats;
- use night settings for comfort, while recognizing that dimmer screens do not solve the problem of lost time;
- tell friends you do not expect instant late-night responses;
- write down the issue that feels urgent and choose a time to address it tomorrow.

A household rule works better when adults follow it too. A teenager should not be the only person asked to put the screen down while everyone else keeps scrolling.

Curate the Feed Instead of Blaming Yourself

Use the controls you have:

- unfollow, mute, block, or mark content as not interested;
- disable autoplay when possible;
- leave groups built around humiliation, crisis competition, or constant conflict;
- turn off recommendation categories that repeatedly lead somewhere harmful;
- follow sources that add context rather than only intensity;
- avoid hate-watching, which still teaches a system to show more;
- create separate accounts for hobbies when that produces healthier recommendations;
- periodically reset recommendations or clear activity where the service provides that option.

You can also add friction. Move the app off the home screen. Log out after use. Use the web version instead of the app. Set a timer that asks a question—"What did I open this for?"—rather than only locking the device.

Comparison, Metrics, and Performance

Follower counts, likes, views, rankings, and streaks convert social life into numbers. Metrics can be useful for creators and teams, but they are incomplete measurements. A post may receive little engagement because of timing, audience, or platform distribution—not because the person who made it lacks value.

Try separating creation from measurement. Make the art, video, post, or stream. Wait before checking statistics. Decide in advance how often analytics will be reviewed. Hide public like counts if that helps. Share important work directly with people who can give thoughtful feedback.

For creators, harassment and burnout can become occupational risks. Establish moderation rules, blocked-word lists, trusted moderators,

and off-camera time before growth makes those boundaries harder to build.

Disturbing Content and Crisis Exposure

Feeds can expose people to violence, self-harm, eating-disorder content, hate, sexual exploitation, disasters, or graphic news without warning. Repeated exposure can increase distress, especially when the content connects to personal experience.

Do not keep watching to prove you are strong. Close the content, ground yourself in the physical room, and talk to someone. Use platform reporting and content controls. Journalists, moderators, advocates, and students researching difficult topics should schedule breaks and avoid unnecessary replay.

When someone posts that they may harm themselves, take it seriously. You do not need to determine whether the post is "real enough." Contact a trusted adult, use the platform's crisis-reporting tool, and call emergency services when there is immediate danger. In the United States, call or text **988** or use the 988 Lifeline chat for crisis support.[17]

Do not promise to keep suicidal intent secret. Caring about someone can include involving people who can provide immediate help.

Taking a Break Without Disappearing

A break can be five minutes, one evening, a weekend, or longer. Tell close friends how to reach you if disappearing would worry them. Save needed contacts. Pause rather than delete an account when you are unsure. Avoid announcing a dramatic departure if that will invite arguments.

A useful break has a replacement: sleep, movement, music, a game played locally with friends, reading, making something, time outside, therapy, or a conversation. Removing an app without addressing loneliness or stress may leave the original need untouched.

Scenario: Jordan Changes the System, Not Just the Goal

Jordan says every morning that he will stop gaming by midnight. Every night, his team starts “one last match” at 11:55. He sleeps through class and feels guilty.

Instead of repeating the promise, Jordan changes the setup. He tells teammates that his final queue begins at 10:45, schedules the console’s downtime, moves the headset out of his bedroom, and asks a friend not to invite him after the cutoff. He also talks with a counselor about why nighttime gaming is his main escape from daytime anxiety.

The boundary works because it is social, technical, and connected to the real problem.

Make It Stick

MEMORY ANCHOR Change the system before blaming yourself.

Pressure Test

You plan to stop scrolling at midnight, but the phone stays beside your pillow, notifications continue, friends expect instant replies, and the feed becomes more intense as you get tired.

A. Rely on more willpower tomorrow.

B. Delete every account during a bad night.

C. Change the environment: charging location, notification schedule, app limits, friend expectations, and the content signals feeding the loop.

BEST FIRST MOVE C. A system that removes cues and frictionlessly supports the desired behavior is more reliable than a promise made while rested.

60-Second Drill

Protect tonight’s sleep: choose a device parking place, set a do-not-disturb schedule, hide lock-screen previews, and tell one friend what “offline” means. Notice the result tomorrow rather than judging yourself tonight.

Say It Out Loud

I am offline until tomorrow. Nothing is wrong between us. I do not expect an immediate reply from you either.

Close the Book: Recall

Before reading the summary, cover the page and answer from memory:

1. Name three signs that online use is affecting functioning.
2. Why is comparison online structurally unequal?
3. When does a break need professional support rather than only app changes?

Chapter 13 Summary

- Online life can provide meaningful connection and also create pressure, sleep loss, compulsive use, or harmful comparison.
- Recommendation systems learn from attention, including negative attention.
- Protecting sleep is one of the highest-value changes.
- Curating feeds and adding friction can reduce unwanted patterns.
- Metrics are incomplete measurements, not measures of human worth.
- Disturbing content and self-harm threats require support, not secret-keeping or repeated exposure.
- Sustainable change addresses the need underneath the habit.

Chapter 13 Safety Checklist

- ☐ Identify which apps or activities improve your life and which usually leave you worse.
- ☐ Set a realistic sleep boundary and allow emergency contacts through Do Not Disturb.
- ☐ Turn off nonessential notifications and autoplay where possible.
- ☐ Unfollow, mute, block, or retrain recommendations that repeatedly cause harm.
- ☐ Create stopping points for games, feeds, and group chats.

- ☐ Tell someone when online activity affects eating, sleep, school, self-harm thoughts, or safety.
- ☐ Treat crisis posts seriously and involve trusted adults or emergency support.
- ☐ Replace breaks with connection, rest, creativity, movement, or professional help.

Chapter 13 Discussion Questions

1. Which platform features make stopping difficult, and what stopping points could replace them?
2. How can a feed change a person's sense of what is normal?
3. What is the difference between a useful break and avoidance?
4. When should a friend's crisis post be shared with an adult despite a request for secrecy?
5. What technology boundary would work better if the adults in a household followed it too?

CHAPTER 14

When Something Goes Wrong—Incident Response for Real People

> ***QUICK RECALL - Do not look back:*** *What should you change before blaming willpower?* ***Check:*** *The environment: notifications, bedtime access, feed signals, and social expectations.*

A security incident is any event that threatens an account, device, identity, privacy, money, reputation, or physical safety. It may be a stolen phone, a suspicious login, a sent photo, a clicked link, malware, impersonation, doxxing, or a scam payment.

The first minutes after an incident can feel chaotic. A simple response model keeps panic from making the next decision.

The Five-Step Response: Safe, Save, Contain, Recover, Learn

1. Safe

Handle immediate human safety first.

- Move away from a person who is threatening you.
- Do not meet an online contact to “settle” a dispute.
- Call emergency services for immediate danger.
- Tell a trusted adult when stalking, sexual exploitation, self-harm, threats, weapons, or a missing person may be involved.
- Use another safe device if you believe yours is being monitored.

2. Save

Preserve enough evidence to explain what happened.

- Take screenshots that include the username, date, time, full message, and surrounding context.
- Copy profile and post links.
- Record transaction IDs, phone numbers, email addresses, account names, and payment details.
- Write a short timeline while events are fresh.
- Save original files when safe; forwarding or repeatedly downloading intimate content can create additional harm.
- Do not edit screenshots in a way that removes context. Make a separate redacted copy for ordinary sharing.

Evidence collection should not become endless exposure. Ask a trusted person to help when reviewing content is distressing.

3. Contain

Stop the incident from spreading.

- Disconnect a suspected infected device from Wi-Fi or mobile data if it is actively behaving strangely.
- Change the affected account's password from a known-safe device.
- Sign out other sessions.
- Remove unfamiliar recovery emails, phone numbers, devices, forwarding rules, and connected apps.
- Freeze or lock payment cards when financial information may be exposed.
- Tell contacts not to trust recent messages from a compromised account.
- Block an abuser after preserving evidence.

Containment is not the same as deleting everything. Deletion can destroy evidence or make recovery harder.

4. Recover

Restore safe access and correct the damage.

- Use the service's official account-recovery page, reached through its app or a manually typed address.

- Update passwords on other accounts that reused the same password.
- Enable MFA or passkeys.
- Restore from a known-good backup when malware or destructive changes are involved.
- Ask the bank, payment service, school, platform, or employer to reverse or document unauthorized activity.
- Report impersonation, abusive content, or exploitation through the correct channel.
- Monitor statements and login alerts.

5. Learn

Once the emergency is stable, identify what will reduce the chance or impact of a repeat.

- Was a password reused?
- Did a recovery email belong to an old account?
- Did urgency or fear override verification?
- Were location details public?
- Did an app have unnecessary permissions?
- Was there no trusted adult or reporting plan?
- Which backup, alert, or boundary would have helped?

Learning is not blaming. A good review improves the system without declaring that the victim "should have known better."

Playbook: You Clicked a Phishing Link

Clicking a link is not automatically a disaster. The response depends on what happened next.

If you only opened the page: close it. Do not download anything or allow notifications. Update the browser and device. Run the device's built-in or trusted security scan. Watch for unusual behavior.

If you entered a password: go to the real service from a bookmark or manually typed address. Change the password immediately from a

safe device. Sign out other sessions. Enable MFA. Change any other account using the same password.

If you entered a verification code or approved a login: treat the account as compromised. Change credentials, review sessions and recovery methods, and contact official support.

If you entered card or bank information: contact the financial institution using the number on the card or official app. Lock or replace the card and monitor transactions.

If you installed software or a mobile profile: disconnect the device from networks, tell an adult or IT administrator, and obtain qualified technical help. Do not rely on deleting the visible app if deeper access may have been granted.

Report phishing to the impersonated organization and, in the United States, to the FTC at ReportFraud.ftc.gov. Significant internet-enabled crimes can be reported to the FBI's Internet Crime Complaint Center at IC3.gov.[3][18]

Playbook: Your Account Was Taken Over

Signs include password-reset notices you did not request, messages you did not send, new followers, changed recovery information, unknown sessions, or friends receiving money requests.

1. Use official account recovery.
2. Secure the email account first if it controls recovery for other accounts.
3. Change the password to a unique one.
4. Remove unknown sessions, recovery methods, forwarding rules, and connected apps.
5. Enable MFA and save recovery codes offline.
6. Warn contacts through another channel.
7. Review posts, messages, purchases, advertising accounts, and privacy settings.
8. Save evidence of fraud, threats, or impersonation.

9. Report unauthorized charges and relevant crimes.

Do not pay someone in a direct message who claims to be a "recovery hacker." Account-recovery scams often target people who have already been harmed.

Playbook: Your Phone Is Lost or Stolen

From another device:

- use the official device-finding service to locate, lock, or mark it lost;
- do not travel alone to confront someone at the displayed location;
- contact the carrier to suspend service or protect the number;
- change the primary email password if the phone was unlocked or poorly protected;
- remove payment cards from the device wallet when appropriate;
- notify school, work, or family if sensitive access is involved;
- file a police report for theft when appropriate, including the device serial number or IMEI;
- remotely erase only after considering whether location, evidence, insurance, or recovery needs require waiting.

When you recover the device, verify that no new profile, app, account, or forwarding rule was added.

Playbook: You Think Someone Is Monitoring Your Device

Possible signs include an abuser knowing private conversations, unexpected account alerts, unfamiliar location sharing, unknown device-management profiles, or settings that repeatedly change. Battery drain alone is not proof of spyware.

Safety comes before technical cleanup. If a controlling person may react violently when access disappears, use a safe device to contact a domestic-violence advocate, trusted adult, or law enforcement. Changing settings may alert the person.

From a safe device:

- review account sessions and location-sharing services;
- check family-plan, cloud, and carrier access;
- examine installed apps, accessibility permissions, device-administration settings, and configuration profiles;
- change important passwords and recovery information;
- document suspicious settings before removal;
- seek qualified help from a device manufacturer, school IT office, victim-service agency, or reputable technician.

A factory reset can remove some unwanted software but may also erase evidence and will not secure an account that remains compromised. Plan the recovery rather than resetting automatically.

Playbook: Malware or a Suspicious Download

Disconnect the device if files are changing, pop-ups are uncontrollable, the camera activates unexpectedly, or accounts are being accessed. Photograph error messages with another device if possible.

Use built-in security tools or trusted software obtained from the vendor's official source. Update the operating system. Remove suspicious browser extensions. Review downloads and installed programs. Change account passwords from a separate clean device when credential theft is possible.

For a school or work device, stop and contact the administrator. Trying to repair a managed device yourself can destroy logs or violate policy.

Do not call the phone number in a pop-up claiming your device is infected. Legitimate operating-system alerts do not require payment with gift cards, cryptocurrency, or remote access from an unsolicited caller.

Playbook: Money or Identity Information Was Stolen

Act quickly, but use official contact paths.

- Contact the bank, card issuer, payment app, or marketplace.

- Ask whether the transfer can be stopped or disputed.
- Change financial-account credentials and secure the associated email.
- Preserve receipts, messages, wallet addresses, and transaction IDs.
- Tell a parent or guardian when a minor's account or identity is involved.
- Report the scam to the platform and appropriate authorities.
- In the United States, use IdentityTheft.gov for a recovery plan when identity information has been misused.
- Consider a credit freeze with the three major credit bureaus when a Social Security number or sufficient identity data is exposed. A parent or guardian can help freeze a minor's credit file.

No legitimate agency will require payment to "protect" your money by moving it to cryptocurrency, gift cards, or a special government account.

Playbook: Your Address or Private Information Was Posted

Refer to the doxxing steps in Chapter 11. In brief:

1. Save the post and link.
2. Assess threats and who has access to the information.
3. Tell household members and school or work.
4. Remove public records and social posts that reveal routines where possible.
5. Ask the platform and search engine for removal under their sensitive-information policies.
6. Tighten location and account security.
7. Contact law enforcement when threats, stalking, swatting, or attempts to approach the home are involved.

Do not post a public correction that supplies more precise information. "That is not my current address" may confirm that the rest of the attack is close.

Playbook: An Intimate Image or Sextortion Threat

Return to Chapter 8 and use **Stop, Save, Tell, Report**.

- Stop communicating and do not pay.
- Save the threat and account information.
- Tell a trusted adult.
- Report to the platform, NCMEC CyberTipline, and law enforcement as appropriate.[11][19]
- Use Take It Down for qualifying images taken while under eighteen; it creates a digital fingerprint on your device without uploading the image itself.[12]
- Use the platform notice process required under the U.S. TAKE IT DOWN Act for qualifying nonconsensual intimate imagery.[13]

Do not ask friends to search for or send you copies. That spreads the content and may expose them to illegal material.

Create an Incident Record

A useful incident record contains:

- your name and safe contact method;
- date and time discovered;
- what happened in one sentence;
- affected accounts, devices, and people;
- actions already taken;
- usernames, links, transaction IDs, and phone numbers;
- screenshots or original notices;
- immediate safety concerns;
- reports filed and confirmation numbers;
- next follow-up date.

Store the record somewhere the attacker cannot access. A trusted adult can keep a copy.

Scenario: Maya Recovers Her Email Before Her Social Account

Maya's social profile starts sending investment messages. She tries changing the social password, but the attacker resets it again. Her older brother asks which account receives password-reset emails. Maya discovers that her email has an unfamiliar forwarding rule and recovery address.

They secure the email first, remove the forwarding rule, change the password, sign out other sessions, and enable MFA. Then Maya recovers the social account and warns friends. Because she saved the original security alerts, she can explain the sequence to support instead of guessing.

The key was identifying the account that controlled the others.

Make It Stick

MEMORY ANCHOR Safe. Save. Contain. Recover. Learn.

Pressure Test

Your email password was reused, your social account is posting scams, and a friend says the attacker is messaging everyone. You have five tabs open and do not know where to start.

A. Post "I was hacked" and wait for support.

B. Delete the social account first.

C. Secure physical safety and the primary email, preserve evidence, contain sessions and recovery changes, recover linked accounts, then review what failed.

BEST FIRST MOVE C. Incident response is a sequence. Recovering the visible account before the root account can let the attacker take it again.

60-Second Drill

Write a five-line incident card using the words Safe, Save, Contain, Recover, Learn. Under each word, put one action that applies to your primary email and phone.

Say It Out Loud

I need ten calm minutes. We will secure the account that controls the others, save what matters, and work the steps in order.

Close the Book: Recall

Before reading the summary, cover the page and answer from memory:

1. What belongs under each of the five response steps?
2. Why should you avoid erasing a device immediately?
3. Which records help after money or identity theft?

Chapter 14 Summary

- Use the sequence Safe, Save, Contain, Recover, Learn.
- Human safety and trusted support come before account cleanup.
- Preserve enough evidence before deleting, blocking, resetting, or erasing.
- Secure the email or identity account that controls other recovery paths.
- Use official apps, typed addresses, and verified contact numbers.
- Device resets and content deletion can destroy evidence; use them deliberately.
- A post-incident review should improve protection without blaming the person harmed.

Chapter 14 Safety Checklist

☐ Address physical danger and contact emergency help first.

☐ Record the timeline, links, usernames, alerts, and transactions.

☐ Use a known-safe device for password and recovery changes.

- ☐ Secure the primary email account and remove unknown sessions or rules.
- ☐ Contact financial institutions through official channels.
- ☐ Warn contacts when a compromised account may target them.
- ☐ Report exploitation, fraud, threats, or abuse to the correct service.
- ☐ Do not pay unsolicited “recovery” experts.
- ☐ Review what control failed and add one practical safeguard.

Chapter 14 Discussion Questions

1. Why does evidence preservation come before deletion in many incidents?
2. Which account in your life controls recovery for the greatest number of other accounts?
3. When could changing a setting increase danger for someone experiencing stalking or control?
4. What is the difference between containment and recovery?
5. Which details make an incident report easier for a school, platform, bank, or police department to act on?

CHAPTER 15

Reporting Abuse and Helping a Friend

> ***QUICK RECALL - Do not look back:*** *What are the five incident-response steps?*
> ***Check:*** *Safe, save, contain, recover, and learn.*

Reporting is not one button. A useful report reaches the organization with the power and responsibility to act, includes enough evidence, and makes a clear request.

You may report to a platform, school, employer, game administrator, financial institution, child-protection organization, crisis service, or law-enforcement agency. Serious cases often require more than one path.

Choose the Right Reporting Path

Platform or game service: impersonation, harassment, threats, sexual content, nonconsensual images, scams, hacked accounts, hate, doxxing, self-harm content, or underage users in adult spaces.

School: conduct that affects attendance, learning, team participation, safety, access to school systems, or relationships among students—even when some conduct occurred off campus. School authority varies, but safety impacts should still be documented.

Employer or volunteer organization: harassment, threats, exploitation, misuse of organizational systems, or conduct affecting the workplace.

Bank or payment service: unauthorized charges, scams, stolen payment information, account takeover, or suspicious transfers.

NCMEC CyberTipline: suspected online enticement, child sexual exploitation, trafficking, child sexual abuse material, or related conduct involving a person under eighteen in the United States.[19]

FBI Internet Crime Complaint Center: internet-enabled fraud, extortion, account compromise, and other cybercrime. Reports help investigators connect incidents even when an individual loss seems small.[18]

Local law enforcement or emergency services: immediate danger, credible threats, stalking, swatting, assault, missing persons, weapons, or crimes requiring local response.

Crisis and victim services: emotional support, safety planning, sexual-assault support, abuse concerns, dating violence, or suicidal crisis.

What Makes a Report Actionable

A clear report answers:

1. **What happened?** Use one or two factual sentences.
2. **Who was involved?** Include usernames, account links, display names, and known real names.
3. **When did it happen?** Provide dates, times, and time zone when relevant.
4. **Where did it happen?** Identify the app, server, channel, school system, game, or physical location.
5. **What evidence exists?** Attach full-context screenshots, links, transaction records, or witness names.
6. **What is the safety risk?** State threats, age differences, sexual coercion, weapons, location exposure, self-harm, or fear of retaliation.
7. **What action are you requesting?** Removal, account preservation, investigation, no-contact measures, payment reversal, safety planning, or emergency response.

Avoid exaggeration. Accurate descriptions make patterns easier to recognize. Use the platform's most specific category—"nonconsensual intimate image" is more actionable than "I don't like this post."

A Reporting Template

> *On [date and time], account [username/link] sent or posted [brief factual description] on [service/location]. The person involved is believed to be [age or relationship, if known]. The content includes [threat, coercion, private information, sexual content, impersonation, or fraud]. I preserved [screenshots, links, transaction IDs, or messages]. I am concerned about [specific safety impact]. I am requesting [removal, preservation of records, investigation, account restriction, safety plan, or contact]. My safe contact method is [method].*

Do not place highly sensitive evidence in an ordinary email unless the receiving organization instructs you to do so. Use secure upload or reporting systems where available.

Following Up

Save confirmation numbers and automated emails. Record who you spoke with and what they said. If a report is closed without addressing a serious safety issue, appeal through the service, ask for a supervisor, or use another appropriate reporting channel.

A platform's decision not to remove content does not determine whether the conduct is legal, safe, or acceptable at school. Different systems apply different rules.

Do not repeatedly submit identical reports every few minutes. That can slow review or be treated as spam. Add new evidence or escalate through a documented route.

Helping a Friend: Believe, Stabilize, Connect

When a friend tells you about abuse or exploitation, your response can affect whether they seek further help.

Believe: “I’m glad you told me. This is not your fault.” Avoid an interrogation or questions that sound like blame.

Stabilize: Ask whether they are physically safe, whether the person knows their location, and whether there are immediate threats. Help them stop contact and preserve evidence.

Connect: Involve a trusted adult and appropriate service. A friend should not become the only person managing sextortion, stalking, suicidal crisis, or abuse.

Do not promise total secrecy. Say: “I will respect your privacy, but if you are in danger, I need to bring in someone who can help.”

Scenario: Sam Tells the Right Person

Sam’s online friend says an older person has private photos and threatens to send them to school. The friend begs Sam not to tell anyone.

Sam replies, “I won’t post this or tell other students. But I care about you too much to keep it only between us.” Sam asks whether the friend is safe at home, saves the username and threat with permission, and contacts a trusted adult. They help the friend report to the platform and CyberTipline and use Take It Down.

The friend is angry for one evening. Later, they say they could not have handled the threats alone. Sam did not betray the friendship; Sam refused to let secrecy protect the offender.

Do Not Become an Investigator

You can preserve what arrives and report it. Do not pose as a child to trap an offender, arrange a meeting, hack an account, threaten retaliation, or search for additional illegal images. Those actions can increase danger, spread harmful material, interfere with an investigation, or create legal problems.

Let trained investigators and victim-service professionals handle evidence requests and contact with suspected offenders.

Adults, Confidentiality, and Mandatory Reporting

Teachers, counselors, health professionals, coaches, and youth-program staff may have different confidentiality rules. Some are required by law or policy to report suspected child abuse, exploitation, or immediate danger.

Before sharing, you can ask: “What are you required to report, and who would you tell?” In an emergency, do not delay help while searching for a person who can promise secrecy.

A report may lead to questions, family involvement, a school process, or law enforcement. That uncertainty can be frightening. A supportive adult should explain what they know, avoid making promises about outcomes, and keep the young person involved in decisions whenever safety and law allow.

Supporting Someone After the Report

Reporting does not end the emotional impact. Offer specific help:

- sit with them while they make a call;
- help write a timeline;
- go with them to the counselor or office;
- monitor public posts so they do not have to;
- help adjust privacy settings;
- bring food, water, or a charger during a long process;
- ask before touching or hugging;
- continue inviting them to ordinary activities;
- avoid demanding updates.

Do not make the event their identity. Recovery includes ordinary life.

When You Are Afraid of Getting in Trouble

Teenagers sometimes avoid help because they broke a household rule, used an app they were forbidden to use, sent an image, met someone secretly, or lied about their age.

Those choices can be addressed later. Immediate protection comes first. A useful adult response sounds like: “We will deal with the rule separately. Right now, we are going to keep you safe.”

If the first adult reacts with blame, find another safe adult. One poor response does not mean help is unavailable.

Make It Stick

MEMORY ANCHOR Believe. Stabilize. Connect.

Pressure Test

A friend says, “Do not tell anyone, but someone is threatening me.” They refuse to explain and say they will never speak to you again if an adult finds out.

A. Promise total secrecy so they keep talking.

B. Investigate the account yourself before involving anyone.

C. Stay calm, ask about immediate safety, explain that danger cannot remain secret, and involve the safest qualified adult or service with them.

BEST FIRST MOVE C. Support does not mean becoming the only person responsible. The goal is to keep connection while bringing in enough help.

60-Second Drill

Choose three adults or services for three levels of need: ordinary advice, urgent safety, and immediate crisis. Put the names and contact routes in your phone and on paper.

Say It Out Loud

I care about you too much to handle danger alone. I will stay with you while we choose the safest adult or service together.

Close the Book: Recall

Before reading the summary, cover the page and answer from memory:

1. What makes a report actionable?
2. What should a helper avoid doing with harmful material?
3. When must safety override a promise of secrecy?

Chapter 15 Summary

- Report to the organization that can act: platform, school, bank, child-protection organization, crisis service, or law enforcement.
- Actionable reports state what happened, who, when, where, evidence, safety risk, and requested action.
- Save confirmation numbers and follow up through documented escalation paths.
- Help a friend by believing, stabilizing, and connecting—not investigating.
- Do not promise secrecy when someone is in danger.
- Rule violations and embarrassment should be addressed separately from immediate safety.

Chapter 15 Safety Checklist

- ☐ Choose the reporting path that matches the harm.
- ☐ Use factual language and the most specific report category.
- ☐ Include dates, links, usernames, context, and requested action.
- ☐ Store confirmation numbers and a follow-up record.
- ☐ Ask about immediate danger, location exposure, and self-harm.
- ☐ Involve a trusted adult in exploitation, stalking, or credible threats.
- ☐ Do not confront, hack, trap, or investigate the suspected offender.
- ☐ Continue supporting the person after the report.

Chapter 15 Discussion Questions

1. Why might a serious incident need reports to more than one organization?
2. What makes a factual report stronger than an emotionally intense but vague report?
3. When is breaking a promise of secrecy justified?
4. Why should friends avoid conducting their own investigation?
5. What can an adult say that separates a broken rule from a safety emergency?

PART IV CHECKPOINT

The Friday Night Pileup

Real incidents overlap. This final simulation is designed to test sequence under pressure.

> **RULE** Choose the safest first move, not the action that solves everything at once.

The Situation

At 11:40 p.m., your friend messages: “Do not call me. Someone has my picture.” At the same time, your own social account sends scam links, an unknown login appears in your email, and a group chat posts your friend’s school schedule. Your friend says they paid once and now the person wants more.

Step 1 - Safe

What immediate physical and emotional safety questions must be answered before account cleanup?

Step 2 - Save

What evidence should be preserved without forwarding or downloading unnecessary harmful content?

Step 3 - Contain

Which account should be secured first, and what sessions or recovery details should be checked?

Step 4 - Connect

Who needs to be involved tonight, and what should you say to your friend?

Step 5 - Report and Recover

Which reports and recovery actions can begin after immediate safety is stable?

Step 6 - Learn

What changes tomorrow reduce the chance that one compromise spreads again?

Answer Key and Reasoning

1. Ask whether your friend is physically safe, alone, being threatened with in-person harm, or thinking about self-harm. Bring in a trusted adult immediately; use 911 or 988 when indicated. Do not obey “do not call” when life or physical safety may be at risk.

2. Save usernames, profile links, message text, dates and times, the payment demand and receipt, URLs showing the posted schedule, login alerts, and report numbers. Do not circulate the intimate image.

3. Secure the primary email first because it can reset other accounts. Deny the unknown login, change reused credentials, sign out other sessions, restore recovery information, inspect forwarding rules, and enable strong MFA.

4. Involve a calm trusted adult for each teen. Say: “You are not in trouble for asking for help. Do not pay or send more. I am staying with you while we save what matters and report it.” Do not become the only helper.

5. Report exploitation to the platform and NCMEC CyberTipline; use Take It Down when eligible; report the schedule post as doxxing and involve the school or law enforcement based on threat; contact the payment provider; recover the social account through official channels; warn contacts elsewhere.

6. Replace reused passwords, review linked apps and devices, preserve recovery codes, reduce live schedule exposure, create a family

verification method, rehearse the incident card, and agree on a no-shame reporting plan.

Teach It Back

Explain the checkpoint to another person in sixty seconds. Use the memory anchors, not the chapter titles. If you cannot explain the first move without looking, review only the section you missed and try again tomorrow.

Emergency and Reporting Resources

This section is primarily for readers in the United States. Services, age rules, and reporting duties vary by location. Outside the United States, contact local emergency services, a national child-protection hotline, or a trusted adult who can locate the correct service. Websites may update their contact methods, so use the official site when a listed method does not work.

Immediate Danger

Emergency services — 911 in the United States Call when someone is in immediate physical danger, a credible threat is unfolding, a person is missing, a weapon is involved, or urgent medical help is needed. Share the location first. Do not travel to confront a suspect.

988 Suicide & Crisis Lifeline Call or text **988**, or chat at **988lifeline.org**. The service supports people experiencing suicidal thoughts, emotional distress, or concern about someone else.[17] If a person is in immediate danger, call emergency services.

Child Sexual Exploitation, Grooming, and Sextortion

NCMEC CyberTipline Report suspected online enticement, child sexual exploitation, child sexual abuse material, trafficking, or related conduct involving a person under eighteen at **report.cybertip.org** or through **missingkids.org/gethelpnow/cybertipline**.[19]

Take It Down At **takeitdown.ncmec.org**, a person can create a digital fingerprint, or hash, of a nude, partially nude, or sexually explicit image or video taken while they were under eighteen. The image remains on the person's device; participating platforms can use the

hash to detect matching copies. The service is available worldwide and can be used anonymously.[12]

Do not download or ask someone to resend an image merely to use the service. Use only a file already on your device.

Sexual Assault, Abuse, and Dating Violence

RAINN National Sexual Assault Hotline Call **800-656-HOPE (4673)**, text **HOPE** to **64673**, or use chat through **rainn.org** for confidential support and referrals.[20]

Childhelp National Child Abuse Hotline Call or text **800-422-4453** or visit **childhelphotline.org** for support related to child abuse and safety.[21]

love is respect Call **866-331-9474**, text **LOVEIS** to **22522**, or chat through **loveisrespect.org** for support involving dating relationships, control, threats, or abuse.[22]

A service's confidentiality and reporting obligations can depend on age, location, and danger. Ask what information may need to be shared.

Fraud, Account Crime, and Identity Theft

FTC ReportFraud Report scams and fraud at **ReportFraud.ftc.gov**. Reports help enforcement agencies identify patterns, even when money is recovered through another provider.[3][6]

FBI Internet Crime Complaint Center Report internet-enabled crime at **IC3.gov**. Preserve usernames, links, payment records, wallet addresses, transaction IDs, and messages.[18]

IdentityTheft.gov Use **IdentityTheft.gov** to create a U.S. identity-theft recovery plan. A parent or guardian may need to assist when a minor's identity is involved.

Your financial institution Use the official app, the number printed on the card, or a verified statement. Do not call a number supplied by the suspected scammer or a search advertisement without verifying it.

Platform, School, and Community Support

Use the platform's dedicated categories for hacked accounts, impersonation, doxxing, credible threats, self-harm, scams, or nonconsensual intimate images. Save the report number.

At school, consider a counselor, principal, school resource officer, Title IX coordinator, team coach, trusted teacher, or district safety contact depending on the issue. Ask for a written safety plan when harassment affects attendance or access.

A trusted adult may be a parent, guardian, relative, counselor, coach, faith leader, healthcare professional, youth worker, or another adult who takes safety seriously. If the first person blames or dismisses you, tell someone else.

What to Have Ready

When it is safe, collect:

- your safe contact information;
- the service, server, channel, or location involved;
- usernames and profile links;
- dates, times, and time zone;
- screenshots with context;
- transaction IDs or receipts;
- a one-paragraph timeline;
- immediate safety concerns;
- previous report numbers;
- the action you are requesting.

You do not need a perfect evidence package before asking for emergency help.

Glossary

Account recovery: The process for restoring access after a forgotten password, lockout, or takeover. Recovery methods can include email, phone, passkey, recovery code, or identity verification.

Account takeover: Unauthorized control of an account, often through stolen credentials, phishing, malicious recovery changes, or session theft.

Algorithm: A defined process used to make decisions or predictions. Recommendation algorithms select content based on signals such as viewing, pausing, sharing, and searching.

Artificial intelligence (AI): Computer systems designed to perform tasks associated with prediction, language, images, decisions, or other forms of pattern processing. AI output can be useful and still be inaccurate.

Authenticator app: An application that produces time-limited codes or receives secure login prompts. It is usually stronger than relying only on text-message codes.

Backup: A separate copy of important information that can be restored after loss, theft, failure, or malware. A backup should not be accessible only through the same compromised account.

Block: A platform control that limits another account's ability to contact or interact with you. Blocking does not remove evidence or guarantee that the person cannot create a new account.

Bot: Software that performs automated actions. Bots may be helpful, spammy, deceptive, or malicious.

Catfishing: Using a false or substantially misleading online identity to form a relationship, gain trust, or manipulate someone.

Child sexual abuse material (CSAM): A legal and victim-centered term for images or videos depicting sexual abuse or exploitation of a

child. It is not “child pornography,” because a child cannot consent to being used in pornography.

Content credential: Information attached to or associated with media to describe its origin or editing history. Credentials can add evidence but do not prove every claim about the content.

Credential stuffing: Automated attempts to log in using username-and-password combinations stolen from other services. Reused passwords make this attack effective.

Cyberbullying: Bullying carried out through digital devices or services. It may include harassment, rumor-spreading, humiliation, impersonation, exclusion, threats, or image abuse.[14]

CyberTipline: NCMEC’s U.S. reporting system for suspected child sexual exploitation and related conduct.[19]

Data broker: A company that collects, combines, analyzes, or sells information about people from multiple sources.

Deepfake: Synthetic or manipulated media that realistically depicts a person saying or doing something that did not occur. Not every edit is a deepfake, and not every deepfake is used maliciously.

Digital footprint: The information created, shared, inferred, or stored through a person’s online activity.

Digital fingerprint or hash: A value calculated from a file. Matching hashes can help services identify known copies without relying only on filenames. NCMEC’s Take It Down uses hashes generated on the user’s device.[12]

Disinformation: False or misleading information created or spread deliberately to deceive. Compare with misinformation.

Doxxing: Publishing or distributing private identifying information to intimidate, harass, locate, or endanger someone.

Encryption: A method of transforming readable information so that only authorized parties with the proper key can access it.

End-to-end encryption: A design in which message content is encrypted so that only communicating endpoints are intended to read it. It does not prevent recipients from taking screenshots or sharing content.

Grooming: A pattern of building trust, secrecy, access, dependence, or sexualized contact to exploit a young person.

Impersonation: Pretending to be another person or organization, often through a copied profile, deceptive account, spoofed address, or AI-generated media.

Incident response: Organized actions used to protect safety, preserve evidence, contain harm, recover access, and reduce repeat risk.

Location metadata: Information about where a photo, device, or activity occurred. It may be embedded in a file or stored separately by an app or service.

Malware: Software designed to damage, disrupt, spy, steal, extort, or gain unauthorized access. Types include ransomware, spyware, and trojans.

Metadata: Information about information, such as time created, device type, sender, file format, or location. Metadata may reveal facts not visible in the content itself.

Multifactor authentication (MFA): Login protection requiring more than one type of proof, such as a password plus a device, app, security key, or biometric. Stronger factors reduce damage from stolen passwords.[2]

Misinformation: False or inaccurate information shared without necessarily intending to deceive. Compare with disinformation.

Nonconsensual intimate imagery (NCII): Nude, sexual, or intimate images shared or created without the depicted person's consent. This includes some AI-generated or altered images under applicable laws and policies.

Passkey: A modern sign-in credential based on public-key cryptography. Passkeys are generally resistant to ordinary phishing because they are bound to the legitimate service.[1]

Password manager: Software that generates and stores strong, unique passwords. Protect the manager with a strong master credential and available MFA.[1]

Phishing: A deceptive attempt to obtain credentials, money, codes, files, or access by impersonating a trusted person or organization.[3]

Private browsing: A browser mode that limits local history and cookie retention after the session. It does not make the user anonymous to websites, networks, or account providers.

Recovery code: A one-time or limited-use code for restoring access when a normal MFA device is unavailable. Store recovery codes somewhere secure and separate from the device they protect.

Reverse-image search: A search using an image rather than text to find matching or visually similar copies online.

Scam: A deceptive scheme intended to obtain money, information, access, labor, or another benefit.

Security key: A physical device used to authenticate a login. FIDO/WebAuthn security keys can provide phishing-resistant MFA.[1]

Session: A period in which a service recognizes a logged-in device. Stolen session tokens may allow access even without the password until the session is revoked.

Sextortion: Threatening to share sexual or intimate content—or claiming to possess it—to demand money, additional content, contact, or compliance.[11]

SIM swapping: Fraudulently transferring a phone number to a new SIM or carrier account, potentially allowing interception of calls and text-message codes.

Social engineering: Manipulating a person into providing information, access, money, or action. Common tools include urgency, authority, fear, curiosity, and affection.

Spoofing: Faking identifying information, such as caller ID, an email sender, a website appearance, or a display name.

Spyware: Software that secretly monitors activity or collects information. In abusive relationships, monitoring may also occur through ordinary accounts, cloud access, or location-sharing settings rather than specialized spyware.

Swatting: Making a false emergency report intended to send an armed police response to a person's location.

Two-factor authentication (2FA): A form of MFA using two factors. The terms are often used interchangeably in everyday conversation.

Verification code: A temporary code used to confirm a login or action. Anyone asking for a code they triggered may be trying to enter your account.

Virtual private network (VPN): A service that encrypts traffic between a device and the VPN provider and changes where traffic appears to enter the internet. A VPN does not guarantee anonymity, stop phishing, or protect an account whose credentials are stolen.

Watermark: A visible or invisible mark intended to identify ownership, origin, or modification. Watermarks can be removed or copied and should not be treated as complete proof.

WebAuthn: A web authentication standard used by passkeys and security keys to provide strong, origin-bound login protection.[1]

The 30-Day Digital-Safety Challenge

This challenge turns the book into small actions. Most days take ten to twenty minutes. Do not rush through a dangerous situation merely to complete a task. Ask a trusted adult for help with accounts, financial information, exploitation, threats, or devices that may be monitored.

Keep a private progress note. At the end of each day, write one sentence: **What became safer, and what still needs attention?**

Week 1: Secure the Accounts That Control Your Life

Day 1 — Draw Your Account Map

List your primary email, school account, phone account, social platforms, gaming accounts, cloud storage, financial apps, and any creator or marketplace accounts. Draw arrows from your email or phone number to every account they can recover. Circle the account that controls the most others.

Finish line: You know which account must be protected first.

Day 2 — Secure Your Primary Email

Create a unique password or passkey. Turn on the strongest MFA the service supports. Review signed-in devices, recovery phone numbers, recovery emails, app passwords, and forwarding rules. Remove anything unfamiliar.

Finish line: Your recovery hub has unique credentials and verified recovery methods.

Day 3 — Start or Clean Up a Password Manager

Choose a reputable password manager. Protect it with a strong master credential and MFA. Import or add your most important accounts. Do not store the only copy of recovery codes inside an account they are meant to recover.

Finish line: At least five important accounts have unique stored passwords.

Day 4 — Replace Reused Passwords

Prioritize email, banking, school, cloud, social media, gaming, and shopping. Do not make small variations of one password. Generate unique credentials.

Finish line: Your highest-impact accounts no longer share passwords.

Day 5 — Upgrade MFA

Replace text-message MFA with an authenticator app, security key, or passkey where practical. Never approve a login prompt you did not initiate.

Finish line: At least three major accounts use stronger MFA.

Day 6 — Save Recovery Codes

Generate current recovery codes for important accounts. Store them in a secure offline place or another protected location unavailable to someone holding your phone.

Finish line: Losing one device would not permanently lock you out.

Day 7 — Update Everything

Update the operating system, browser, apps, router firmware if you manage it, and security software. Remove apps and browser extensions you do not recognize or use.

Finish line: Automatic updates are enabled where appropriate.

> **WEEK 1 RECALL CHECK** Without looking back, say why the primary email comes first, name two phishing-resistant login methods, and

explain where recovery codes belong. Then teach the answer to someone else in sixty seconds.

Week 2: Reduce Privacy and Location Exposure

Day 8 — Audit App Permissions

Review camera, microphone, contacts, photos, Bluetooth, local network, accessibility, and location permissions. Choose “while using” or approximate location when full access is unnecessary.

Finish line: No forgotten app has powerful access without a reason.

Day 9 — Check Location Sharing

Review family services, map apps, social platforms, photo maps, fitness apps, games, and device-finding groups. Confirm every person who can see your location.

Finish line: Location sharing is intentional, limited, and understood.

Day 10 — Remove Routine Clues

Inspect public posts and bios for school schedules, bus stops, workplace shifts, team travel, house numbers, license plates, bedroom views, and regular check-ins. Remove what creates avoidable risk.

Finish line: A stranger cannot easily predict tomorrow’s routine.

Day 11 — Review Photo Metadata and Backgrounds

Learn whether your camera stores location data. Check one photo before sharing it. Notice mail, badges, calendars, uniforms, mirrors, windows, and screens in the background.

Finish line: You can explain what a photo reveals beyond its subject.

Day 12 — Clean Connected Apps

Review “Sign in with” connections and third-party access in your major accounts. Remove quizzes, old games, editing tools, and services you no longer use.

Finish line: Fewer companies retain ongoing account access.

Day 13 — Search Yourself

Search your name, usernames, and a public profile photo while signed out. Record impersonation, exposed personal information, and outdated results that need action.

Finish line: You know what a stranger can find quickly.

Day 14 — Set a Sharing Rule

Write a personal rule such as: “I do not post live location,” “I ask before posting friends,” or “I wait until returning home to share trip photos.” Tell one person who can help you keep it.

Finish line: Privacy is a repeatable habit, not a mood.

> **WEEK 2 RECALL CHECK** Without looking back, explain “pieces become a map,” “least access first,” and “post the memory, not the opportunity.” Revisit only the phrase you cannot explain clearly.

Week 3: Improve Judgment Under Pressure

Day 15 — Build a Verification Habit

Choose one rule: call back through a saved number, open the official app instead of a message link, or verify unusual requests through a second channel.

Finish line: Urgency no longer decides the channel you use.

Day 16 — Practice a Phishing Drill

Find a harmless sample phishing message from an official education site. Identify the claimed sender, pressure tactic, requested action, suspicious link, and safe verification method.

Finish line: You can describe the manipulation, not just the typo.

Day 17 — Create a Family or Friend Code Word

Choose a private word or question for urgent calls involving money, rides, arrest claims, or AI-cloned voices. Do not use information visible on social media.

Finish line: A frightening voice message must pass independent verification.

Day 18 — Review Payment Risks

Learn how your payment apps handle disputes. Turn on transaction alerts. Remove expired cards and unfamiliar devices. Agree never to pay a stranger with gift cards or cryptocurrency to solve an emergency.

Finish line: You know whom to contact before sending money.

Day 19 — Test a Claim

Choose a viral claim. Find the earliest available source, check the date, search for independent reporting, inspect context, and distinguish evidence from commentary.

Finish line: You can explain why the claim is supported, uncertain, or false.

Day 20 — Audit AI Trust

List three tasks for which AI output must be checked—health, legal rules, money, school citations, identity, or breaking news. Decide what authoritative source will verify each.

Finish line: Fluent output no longer receives automatic trust.

Day 21 — Review Online Relationships

Think about online contacts who request secrecy, move platforms quickly, avoid verification, give gifts, demand constant access, sexualize conversation, or punish boundaries. Tell a trusted adult about any pattern that concerns you.

Finish line: Affection does not cancel safety checks.

> **WEEK 3 RECALL CHECK** Recite PAUSE. Then name the three relationship signals: secrecy, escalating proof, and fear or control. Practice the sentence you would use to refuse a verification code, payment, private image, or secret meeting.

Week 4: Build Response and Well-Being Systems

Day 22 — Configure Report and Block Tools

Find the report, block, mute, restrict, comment-filter, and hacked-account tools on your main platforms. Bookmark official recovery pages.

Finish line: You do not need to learn the controls during a crisis.

Day 23 — Make an Evidence Folder

Create a protected folder for incident screenshots, timelines, links, and report confirmations. Do not fill it with unnecessary intimate or illegal content.

Finish line: Evidence can be organized without being redistributed.

Day 24 — Write Your Incident Card

On paper or in a safe note, write: **Safe, Save, Contain, Recover, Learn.** Add official numbers for your bank, carrier, school, trusted adult, and local emergency services.

Finish line: Panic has a written next step.

Day 25 — Protect Sleep

Set a realistic final time for feeds, games, and group chats. Schedule Do Not Disturb while allowing selected emergency contacts. Charge the phone out of reach tonight.

Finish line: One night of sleep is protected by settings and expectations.

Day 26 — Retrain One Feed

Unfollow or mute accounts that repeatedly cause distress. Mark unwanted recommendations. Follow two sources that add skill, context, recovery, or joy.

Finish line: Your attention produces a different signal.

Day 27 — Establish a Friend Protocol

Agree with one friend: no forwarding private images, no posting each other without consent, verify unusual money requests, and involve an adult when someone is in danger.

Finish line: Friendship has safety rules before a crisis.

Day 28 — Identify Three Trusted Adults

Choose three adults in different settings, such as home, school, healthcare, work, or community. Record how to contact them. Consider who may have mandatory-reporting duties.

Finish line: One unavailable or unhelpful adult does not end the search for help.

Day 29 — Run a Scenario

Choose one scenario: stolen phone, hacked email, doxxing, sextortion threat, fake emergency call, or cyberbullying. Walk through what you would save, contain, report, and request.

Finish line: Your plan contains specific actions and official channels.

Day 30 — Write Your Digital-Safety Agreement

Write one page covering:

- what you protect;
- how you verify urgent requests;
- what you never keep secret;
- when you involve an adult;
- your sleep and notification boundary;
- how you treat other people's privacy;
- the first three steps after an incident;
- the date of your next review.

Share it with a parent, educator, mentor, or friend who will respect the agreement rather than use it as surveillance.

Finish line: You have a living plan, not a finished checklist.

FINAL RETRIEVAL CHECK Recite both safety loops without looking. Work one scenario from each part of the book. Schedule a seven-day follow-up to repeat the same check; memory grows when the skill is retrieved again after time has passed.

Final Reflection

1. Which action reduced the greatest risk?
2. Which action was emotionally hardest?
3. What still depends on a parent, school, company, or professional?
4. Which boundary needs support from friends or family?
5. What will you review every month, every three months, and every year?

Safety is not a thirty-day achievement badge. The challenge creates systems that can keep adapting as your accounts, relationships, responsibilities, and technology change.

Parent and Educator Discussion Guide

Teen internet safety works best as a shared responsibility. Adults control many conditions young people cannot: device purchases, school systems, household rules, reporting relationships, transportation, healthcare, and access to professional help. A teenager should not be expected to outsmart every platform, scammer, or offender alone.

Begin With a No-Shame Response

Before an emergency occurs, say clearly:

> *You can come to me even if you broke a rule, clicked the link, met the person, sent the image, or hid the account. We will handle immediate safety first. Consequences, if needed, will be separate and proportionate.*

A no-shame response does not eliminate boundaries. It prevents fear of punishment from becoming an offender's strongest weapon.

Use Questions That Invite Information

Instead of "Why would you do that?" try:

- "What did you believe was happening at the time?"
- "What are you afraid will happen next?"
- "Does this person know where you live or go to school?"
- "What evidence still exists?"
- "Who else knows?"
- "What would help you feel safer tonight?"
- "What am I required to report, and how can I keep you involved?"

Avoid demanding every detail at once. Repeated retelling can increase distress and produce inconsistencies that are normal under stress.

Facilitate the Scenarios

For each fictional scenario, ask learners to identify:

1. the first warning sign;
2. the moment pressure changed the decision;
3. the safest next action;
4. the evidence worth preserving;
5. the person or organization able to help;
6. the design feature or social expectation that increased risk;
7. how an adult could respond without blame.

Do not ask students to disclose personal victimization in a group. Provide a private reporting path and explain confidentiality limits before discussion.

Create a Household or Classroom Response Contract

A practical contract can include:

- immediate safety before punishment;
- adults will not publicly retell the incident;
- evidence will be handled carefully;
- private images will not be forwarded for proof;
- devices will not be confiscated automatically when they are the person's access to support;
- sleep, location, and posting rules apply consistently;
- adults will explain reports and next steps when possible;
- the plan will be reviewed as maturity and circumstances change.

Device removal may sometimes be necessary, but it can also isolate a victim, destroy evidence, interrupt school, or make reporting harder. Match the response to the actual risk.

School and Program Preparation

Schools and youth programs should maintain:

- clear reporting routes for students and families;
- preservation procedures for platform and school-system evidence;
- a response plan for doxxing, swatting, sextortion, impersonation, and account compromise;
- staff training on mandatory reporting and trauma-informed response;
- crisis and victim-service contacts;
- accommodations and safety planning that protect continued access to education;
- rules addressing retaliation and redistribution of harmful content;
- age-appropriate media-literacy and security education.

Policies should distinguish ordinary conflict from bullying, credible threats, discrimination, sexual exploitation, and criminal conduct. One label cannot produce the right response to every harm.

When Professional Help Is Needed

Seek qualified help when online activity is connected to self-harm, suicidal thoughts, trauma symptoms, eating problems, severe sleep disruption, stalking, coercive control, sexual abuse, threats, or major functional decline. Digital settings may contribute to the problem, but deleting an app is not a substitute for mental-health care, victim services, medical care, or law enforcement when those are needed.

Closing Message for Adults

The goal is not complete control over a teenager's digital life. It is a relationship strong enough that danger can be disclosed early, skills strong enough to reduce ordinary risk, and systems strong enough to respond when individual judgment is not enough.

Sources and Further Reading

The numbered references below correspond to citations in the text. All web resources were reviewed for this edition in July 2026. URLs and services can change; use the organization's official homepage if a link is moved.

[1] National Institute of Standards and Technology. *Digital Identity Guidelines: Authentication and Authenticator Management, NIST SP 800-63B-4.* July 2025. Password length, password-manager support, passkeys, WebAuthn, and phishing-resistant authentication. Open NIST password guidance

[2] Cybersecurity and Infrastructure Security Agency. *Secure Our World.* Guidance on strong passwords, multifactor authentication, software updates, and phishing recognition. Open CISA guidance

[3] Federal Trade Commission. *How To Recognize and Avoid Phishing Scams.* Open FTC consumer guidance

[4] Federal Trade Commission. Consumer guidance on online privacy, social media, advertising, and protecting personal information. Open FTC consumer guidance

[5] National Security Agency. *Limiting Location Data Exposure* and mobile-security guidance, updated April 2026. Open NSA mobile-security guidance

[6] Federal Trade Commission. Consumer scam guidance, including social-media, romance, payment, and impersonation scams. Open FTC consumer guidance

[7] National Institute of Standards and Technology. *AI Risk Management Framework* and *Generative Artificial Intelligence Profile, NIST AI 600-1.* Open NIST guidance

[8] Federal Trade Commission. Consumer guidance on voice cloning and impersonation scams. Open FTC consumer guidance

[9] UNESCO. *Media and Information Literacy.* Skills for evaluating media, misinformation, disinformation, hate speech, and AI-influenced information environments. Open UNESCO media-literacy guidance

[10] National Center for Missing & Exploited Children. *Online Enticement.* Open NCMEC source

[11] Federal Bureau of Investigation. *Sextortion* and *Financially Motivated Sextortion.* Open FBI guidance

[12] National Center for Missing & Exploited Children. *Take It Down.* Open NCMEC Take It Down

[13] Federal Trade Commission. TAKE IT DOWN Act consumer and compliance guidance, including the May 19, 2026 platform notice-and-removal requirements. Open FTC consumer guidance Open FTC TAKE IT DOWN guidance

[14] StopBullying.gov. *What Is Cyberbullying* and reporting guidance. Open StopBullying.gov guidance

[15] Office of the U.S. Surgeon General. *Social Media and Youth Mental Health.* Open HHS youth-safety guidance

[16] Office of the U.S. Surgeon General. *Warning on the Harms of Screen Use,* 2026. Open HHS youth-safety guidance

[17] 988 Suicide & Crisis Lifeline. Youth resources and call, text, and chat support. Open 988 Lifeline resources

[18] Federal Bureau of Investigation. *Internet Crime Complaint Center.* Reporting and public-service guidance on internet-enabled crime. Open FBI IC3 source

[19] National Center for Missing & Exploited Children. *CyberTipline.* Open NCMEC source Open the NCMEC CyberTipline report form

[20] RAINN. *National Sexual Assault Hotline.* Open RAINN resources

[21] Childhelp. *National Child Abuse Hotline.* Open Childhelp resources

[22] love is respect. Confidential support for teens, young adults, and loved ones regarding healthy relationships and dating abuse. Open love is respect resources

[23] Federal Trade Commission and NCMEC. Consumer education on gaming purchases, advertising, privacy, and online safety. Open FTC consumer guidance Open NCMEC source

[24] FBI Internet Crime Complaint Center. Public alerts on online gaming, violent online networks, sextortion, swatting, SIM swapping, and youth-targeted extortion. Open FBI IC3 source Open FBI IC3 source

[25] Federal Trade Commission. Children's Online Privacy Protection Act resources. Open FTC source

[26] Federal Trade Commission. *Image-Based Abuse: What To Know and Do.* Open FTC consumer guidance

[27] Karpicke, J. D., and Roediger, H. L. III. The Critical Importance of Retrieval for Learning. Science, 2008. Repeated retrieval and long-term retention. PubMed PMID 18276894.

[28] Cepeda, N. J., Pashler, H., Vul, E., Wixted, J. T., and Rohrer, D. Distributed Practice in Verbal Recall Tasks: A Review and Quantitative Synthesis. Psychological Bulletin, 2006;132(3):354-380. Spacing and long-term retention. doi:10.1037/0033-2909.132.3.354.

[29] Wisniewski, P. and colleagues. Research on adolescent online-safety resilience and self-regulation, including Parental Control versus Teen Self-Regulation and subsequent teen-centered safety work. Used as a design basis for agency, transparent support, and coping skills.

[30] National Center for Missing & Exploited Children. NCMEC Releases New Sextortion Data: More Than 50,000 Reports in 2025, Averaging 137 Per Day. June 25, 2026. https://www.missingkids.org/blog/2026/ncmec-releases-new-sextortion-data-2025

Editorial Note

This book provides education and general safety planning, not legal, medical, mental-health, or forensic advice. Laws and platform rules differ by jurisdiction and change over time. In an emergency, contact qualified local help.

Closing: Connection Without Surrender

Being safe online does not require surrendering curiosity, friendship, humor, creativity, privacy, or independence. It requires understanding that digital spaces are built environments. They have doors, cameras, crowds, incentives, blind spots, and emergency exits—even when those features are hidden behind a smooth screen.

You will make mistakes. So will adults, companies, schools, and people you trust. The measure of safety is not whether nothing bad ever happens. It is whether you can recognize pressure, protect what matters, ask for help without shame, and recover without handing the rest of your life to the person who caused the harm.

Stay connected. Keep your boundaries. Verify what demands urgency. Protect other people's dignity as seriously as your own. And when something goes wrong, remember: **stop, save, tell, report—then take the next safe step.**

Appendix A: Personal Digital-Safety Plan

Complete this plan privately with a trusted adult, mentor, or educator. Do not write passwords, verification codes, recovery codes, Social Security numbers, or other secrets in the plan.

1. What I Need to Protect

My highest-impact accounts are:

1. _____
2. _____
3. _____
4. _____
5. _____

The email account that controls most recovery links is:

_____

The device that contains the most important information is:

_____

The information that could create the greatest safety risk if exposed is:

_____

Examples may include a home address, routine location, private medical information, financial access, school records, confidential messages, or intimate content.

2. My Trusted-Person Network

Trusted adult at home Name:
_____ Safe contact method:
_____

Trusted adult at school, work, or an activity Name: _____ Safe contact method: _____

Another adult or professional Name: _____ Safe contact method: _____

Before sharing sensitive information, I may ask:

> *What are you required to report, who would you contact, and how can I remain involved in what happens next?*

No single person has to be perfect. If the first adult cannot help, I will contact:

_____

3. My Emergency Verification Rule

When someone urgently requests money, a code, a ride, private information, or secrecy, I will verify through:

_____

My family or friend verification word/question is stored with:

_____

I will never provide a verification code to someone who contacted me unexpectedly, even if the caller ID or account name appears familiar.

4. My Account-Recovery Plan

My recovery codes are stored securely at:

_____

My current recovery email and phone have been checked on this date:

_____

The official recovery pages for my most important services are bookmarked on:

_____

If my primary email is taken over, the first safe device I can use is:

_____

5. My Location and Posting Boundaries

I will not share live location publicly when:

_____

I will wait to post travel, event, or home photos until:

_____

Before posting another person, I will:

_____

People who currently have ongoing location access are:

_____

The next date I will review this list is:

_____

6. My Well-Being Boundaries

My realistic stop time for games, feeds, and group chats on school nights is:

_____

The notifications allowed during sleep are:

_____

Signs that I need help rather than another hour online include:

_____

Activities and people that help me reset are:

_____

If I or a friend may be in suicidal crisis in the United States, I will call or text 988, use 988lifeline.org, involve a trusted adult, or call emergency services for immediate danger.

7. My Incident Plan

Write the five steps from Chapter 14:

1. _____
2. _____
3. _____
4. _____
5. _____

My protected evidence folder is located at:

_____

The official contact number for my bank or payment provider is stored at:

_____

The official contact method for my school or employer is:

_____

For suspected child sexual exploitation, my reporting path is:

_____

For internet-enabled crime, my reporting path is:

_____

For immediate physical danger, I will:

_____

8. My No-Shame Agreement

The adult and teenager completing this plan can adapt the following statement:

> *If I ask for help after breaking a rule, clicking a link, sending content, hiding an account, or trusting the wrong person, immediate safety comes first. We will preserve evidence, stop ongoing harm, and contact appropriate help. Any discussion about rules will happen separately and will not be used to shame me for reporting.*

Teen or learner initials: _____

Parent, guardian, educator, or mentor initials: _____

Date reviewed: _____

Next review date: _____

Appendix B: Scripts for Difficult Moments

The hardest sentence is often the first one. These scripts can be changed to fit your situation.

Telling an Adult About an Online Emergency

> *I need help with something online. I am afraid you will be angry, but I need safety before consequences. Someone is [threatening me / sharing information / controlling an account / asking for money / using an image]. I saved what I could. Can you stay calm and help me decide who to contact?*

Telling an Adult About Sextortion

> *Someone has or claims to have an intimate image of me and is threatening to share it unless I pay or do what they say. I have stopped replying and saved the account information. I need help reporting this. Please do not contact the person directly or forward the image.*

Asking a Friend to Involve an Adult

> *I care about you, and this is bigger than what we can safely handle alone. I will not post it or tell other students, but I cannot promise to keep danger secret. Let's choose an adult together, and I will stay with you while we explain.*

Refusing a Verification-Code Request

> *I do not share login or verification codes. I will contact the company or person through a number or account I already trust.*

No further explanation is required.

Verifying a Strange Message From Someone You Know

> *I received an unusual request from your account. I am checking through a separate channel before I respond. Please confirm what you sent without asking me for a code or payment.*

Ending a Pressuring Online Conversation

> *I am not comfortable with this request. Do not ask again. I am ending the conversation.*

When the person has already ignored a boundary, you do not owe a final warning. Save evidence and block.

Asking Someone to Remove a Post

> *This post includes my [photo / location / private information] and I did not agree to share it. Please remove the post and any copies you control. Do not repost or send it to anyone else.*

For threats or intimate images, preserve evidence and use formal reporting rather than relying only on a request to the poster.

Reporting Impersonation

> *This account is impersonating me. My authentic account is [link, if safe to provide]. The impersonating account uses my [name / photo / school / messages] and is [contacting others / requesting money / posting harmful content]. I am requesting removal and preservation of relevant records.*

Reporting Doxxing to a School

> *On [date], [account or person] posted my private location information and [included threats / encouraged contact / identified my schedule]. This affects my ability to attend safely. I preserved the links and screenshots. I am requesting an immediate safety assessment, preservation of school-system records, protection from retaliation, and a written plan for attendance and contact.*

Correcting Misinformation Without Starting a Fight

> *The available evidence does not support that claim. The original source says [brief correction], and the date/context matters because [reason]. Here is the primary source. I am not going to continue a personal argument.*

Pausing a Late-Night Conflict

> *I am too tired to handle this well. I am not ignoring you. I will return to the conversation after [specific time] when we can talk without an audience.*

A pause is not useful when there is immediate danger. Contact help instead.

Asking a Platform to Preserve Information

> *I am reporting conduct involving [a credible threat / exploitation / account takeover / stalking / fraud]. Please preserve relevant account and access records associated with the reported content in accordance with your procedures. My report confirmation number is [number].*

A platform may require a formal legal request before releasing records, but preservation language can clarify that the incident may require investigation.

Following Up After a Report

> *I submitted report [confirmation number] on [date] regarding [brief description]. The safety risk remains [state risk]. New evidence is attached. Please confirm whether the report has been escalated and what additional information is required.*

Apologizing After Causing Digital Harm

> *I posted or shared [specific action]. It exposed or harmed you by [specific impact]. That was wrong. I removed what I control and asked recipients not to reshare it. I have reported copies where appropriate. I do not expect forgiveness, but I will respect any boundary you set and accept the consequences.*

Do not include excuses, demand a reply, or ask the harmed person to reassure you.

Asking for a Mental-Health Break

> *My online use is affecting my sleep, mood, eating, school, or sense of safety. I do not need only a punishment or total device ban. I need help changing the pattern and understanding what is underneath it. Can we make a plan and contact a counselor or healthcare professional if needed?*

Telling a Friend You Are Going Offline

> *I am taking a break until [time/date]. Nothing is wrong between us. For something truly urgent, contact me through [safe method]. I do not expect immediate replies from you either.*

Final Reminder

A script cannot guarantee a good response. It can help you state the facts and ask clearly for what you need. If someone dismisses danger, blames you, or refuses appropriate help, use another reporting route. Persistence is not overreacting when safety remains unresolved.

Appendix C: Pocket Action Cards

Screenshot or print these cards before you need them. Keep one with a trusted adult. The cards give first moves; the chapters explain the full response.

CARD 1 - PAUSE BEFORE YOU TAP

- PRESSURE - Name the fear, urgency, reward, shame, anger, or belonging being used.
- ASK - What do they want: access, money, an image, location, secrecy, or attention?
- USE ANOTHER CHANNEL - Leave the message. Open the real app, site, or contact yourself.
- SOURCE - Trace who started the claim and what independent evidence confirms it.
- EXIT AND ENGAGE BACKUP - Stop and involve a trusted person when the risk is bigger than you.

CARD 2 - ACCOUNT TAKEOVER

1. Start with the primary email.
2. Change reused passwords through official apps or sites.
3. Sign out unknown sessions and devices.
4. Restore recovery phone, email, passkeys, and MFA.
5. Check forwarding rules, linked apps, purchases, and payment methods.
6. Warn contacts through a different channel.
7. Save login alerts and report confirmations.

CARD 3 - SEXTORTION OR INTIMATE-IMAGE THREAT

- STOP - Do not pay, send more, bargain, or threaten back.
- SAVE - Keep usernames, links, threats, payment demands, dates, and report numbers. Do not forward the image.
- TELL - A trusted adult now. Say: “I need safety before consequences.”
- REPORT - Platform, NCMEC CyberTipline, and law enforcement when appropriate.
- REMOVE - Use Take It Down for eligible images taken before age 18; use the platform’s TAKE IT DOWN Act process for covered content.
- CRISIS - 911 for immediate danger; call or text 988 for emotional crisis or self-harm risk.

CARD 4 - SCAM, PAYMENT, OR VERIFICATION CODE

- Leave the message and open the real account directly.
- Never send a login or verification code requested through a message.
- Contact the bank, card company, payment app, or carrier immediately using official contact information.
- Change exposed passwords, enable MFA, and sign out other sessions.
- Save receipts, transaction IDs, messages, usernames, and URLs.
- Report identity misuse through IdentityTheft.gov and internet crime through IC3 when appropriate.

CARD 5 - DOXXING, HARASSMENT, OR THREAT

- Move to a safe place if the threat could become physical.
- Save the exact URL, account, date/time, screenshots, witnesses, and threat language.
- Do not counter-dox, threaten, or build a public proof thread.
- Reduce exposure: private settings, location off, tags reviewed, school or work notified.
- Report to the platform and the correct school, employer, service, or law-enforcement path.
- Keep a factual incident log and every report number.

CARD 6 - HELPING A FRIEND

- BELIEVE - “I am glad you told me.”
- STABILIZE - Ask about immediate physical safety and self-harm risk.
- CONNECT - Bring in the safest adult or qualified service; do not become the only helper.
- DO NOT - Promise dangerous secrecy, investigate the offender, forward harmful content, or shame the friend.
- STAY - Help with one step at a time and keep the friend involved when safety allows.

CARD 7 - LOST PHONE OR UNKNOWN TRACKER

- Use a safe device to locate, lock, or mark a phone lost. Change critical account access when needed.
- Contact the carrier about SIM or number protection.
- For an unknown tracker, move to a public safe place and save the alert and route.
- Do not confront a suspected person alone.
- In an abusive situation, get specialized safety-planning help before changes that could alert the person.

About This Guide

Connected Without Compromise was designed for independent teen readers, families, classrooms, youth programs, and community discussions. It treats online safety as a combination of security, privacy, media literacy, healthy relationships, mental well-being, and practical incident response. No single setting, application, or household rule can cover all of those areas.

The scenarios are fictional composites. They are intended to make decisions concrete without representing a particular person or case. Readers may recognize parts of their own experiences. That recognition is an invitation to seek support, not proof that they caused what happened.

Technology and law change quickly. This edition reflects authoritative guidance reviewed in July 2026, including the final NIST digital-identity guidelines published in 2025 and the Federal Trade Commission's 2026 enforcement guidance for the TAKE IT DOWN Act. Platform interfaces, reporting categories, telephone services, and legal requirements may change after publication. When a procedure matters, confirm it through the official source listed in the reference section.

A reader does not need to complete every checklist before becoming safer. Start with the risk that could cause the greatest harm:

immediate danger, exploitation, account recovery, location exposure, financial access, or loss of sleep and functioning. Then make the next improvement. Durable safety is usually built through several modest controls, trustworthy relationships, and a response plan that still works when someone is scared.

Return to Contents

For corrections and platform updates, use the Connected Without Compromise update center.