

OPTIONAL REFERENCE HANDOUTS



CYBER BASICS 101

Bonus Reference Packet

Extra handouts for deeper follow-up

These pages are separate from the main presentation packet.
Use them when someone wants more detail, needs a specific topic,
or wants a reference guide to take home.

Prepared by Marc Ortner

Cyber Basics 101
contact@cyberbasics101.com
cyberbasics101.com

CYBER BASICS 101

OPTIONAL REFERENCE HANDOUTS

Table of Contents

How to use this packet

This packet is separate from the main presentation packet.
Use these handouts when a topic comes up or when someone wants more detail.

Inside this optional packet

- 1 Best and Safest Web Browsers**
A plain-English browser comparison for everyday users.
- 2 Secure Messaging Apps**
Private messaging options for iPhone and Android.
- 3 Hidden Apps and Deleted App Clues**
A parent-friendly guide for checking family-owned devices.
- 4 Website and Account Organizer**
A safer way to organize website and app login details.

Reminder

Not every audience needs every extra handout.
Give this packet when it is useful.
Or keep individual copies available on the side.

Extra detail is helpful when people are ready for it.

BEST & SAFEST WEB BROWSERS

Choosing a browser without needing a technology degree, a panic button, or 47 settings menus.

A simple guide for everyday online safety

Start here

A browser helps protect you from risky websites, dangerous downloads, tracking, scam pop-ups, malicious links, and some weak privacy settings. No browser is perfect. The goal is safer, harder to track, and harder to target.

What a good browser should help with

Risk	What the browser can help do
Fake websites	Warn before you land on known phishing or scam pages.
Dangerous downloads	Block or warn about malware and suspicious files.
Tracking	Reduce ad tracking, cross-site tracking, and cookie-based tracking.
Fingerprinting	Make it harder for websites to recognize your device by browser details.
Annoying junk	Block or reduce pop-ups, bad ads, and some malicious scripts.
Oversharing	Give you privacy settings that do not require a computer science degree.

Important reminder

A browser will not stop every scam, every fake message, every bad link, or every bad decision made at 11:47 p.m. while half-asleep. A good browser helps. Your habits still matter more.

MY TOP BROWSER RECOMMENDATIONS

Quick picks first, because nobody should need a spreadsheet just to open the internet.

Best choice by situation

Situation	Pick	Why
Best overall for most people	Brave	Strong privacy by default, blocks a lot of tracking, and does not require babysitting every setting.
Best privacy-focused alternative	Firefox	A trusted browser with strong privacy features and good website compatibility.
Best for Apple users	Safari	Built into iPhone, iPad, and Mac. Simple, secure, and good enough for many everyday users.
Best security and compatibility	Chrome	Strong security warnings and broad website support, but not my first privacy pick.
Best built-in Windows option	Microsoft Edge	Already installed, reasonably safe, and protected by Microsoft Defender SmartScreen.
Best simple private browser	DuckDuckGo Browser	Good for people who want less tracking without tweaking a bunch of settings.
Best for serious anonymity	Tor Browser	Powerful, but not ideal for normal daily browsing. It is a special-purpose tool.
Best advanced privacy browser	Mullvad Browser	Built with the Tor Project to reduce tracking and fingerprinting, especially for advanced users.

My simple answer

For most everyday users, start with Brave. For Apple users who want simple and built in, Safari is fine. For people who want a strong alternative to Google or Microsoft, Firefox is a very good choice.

BROWSER COMPARISON

What each browser is best at

Browser	Best for	Main strength	Trade-off
Brave	Privacy and everyday protection	Blocks many trackers, cross-site cookies, ads, and fingerprinting attempts by default.	Some sites may need small adjustments if blocking is too aggressive.
Firefox	Privacy with a normal browser feel	Enhanced Tracking Protection and Total Cookie Protection help reduce tracking.	May need a few setting changes for stronger privacy.
Safari	Apple users	Strong Apple integration and privacy protections built into the browser.	Best inside the Apple world. Less flexible than Firefox or Brave.
Chrome	Compatibility and security warnings	Google Safe Browsing and Enhanced Protection can warn about harmful sites and downloads.	Strong security, but weaker privacy choice for people avoiding Google tracking.
Edge	Windows built-in safety	SmartScreen helps block phishing, malware sites, and risky downloads.	Convenient, but still not my first privacy pick.
DuckDuckGo	Simple privacy, especially on phones	Blocks many trackers and helps reduce cookie pop-up nonsense.	Less powerful for advanced control than Brave or Firefox.
Tor	Anonymity and censorship resistance	Routes browsing through Tor and resists fingerprinting.	Slower, more blocked sites, and overkill for daily use.
Mullvad	Advanced fingerprinting protection	Designed with the Tor Project to reduce tracking and fingerprints.	Better for advanced users who understand privacy trade-offs

BRAVE AND FIREFOX

1. Brave - best overall choice for most people

Brave is one of the best choices for regular people because it blocks a lot of tracking by default. That matters because most people are not going to dig through 47 browser settings just to stop websites from following them around like a clingy ex.

- Blocks many ads and trackers.
- Helps reduce cross-site tracking.
- Includes fingerprinting protections.
- Gives strong privacy without a complicated setup.

My honest take

For most everyday users, Brave is my top pick. It is simple, private, blocks a lot of junk automatically, and does not require the user to babysit every setting like they are launching a spaceship.

2. Firefox - best privacy-focused alternative from a well-known company

Firefox is a strong choice for people who do not want to rely on Google Chrome or Microsoft Edge. It gives a good mix of privacy, control, and normal website compatibility.

- Enhanced Tracking Protection helps block many trackers.
- Total Cookie Protection keeps cookies separated by site.
- Good balance of privacy and normal website behavior.
- A strong choice for people who want control without making every website act broken.

My honest take

Firefox is a very good choice. I would recommend it to someone who wants privacy but still wants a normal browser experience.

SAFARI AND CHROME

3. Safari - best built-in choice for Apple users

Safari is a strong browser for people who use iPhone, iPad, or Mac. It is already built in, works well with Apple privacy settings, and does not require a confusing setup.

- Works well with iPhone, iPad, Mac, and iCloud Keychain.
- Includes cross-site tracking protections.
- Includes privacy reporting and Apple privacy features.
- Good for people who want safe and simple without installing another browser.

My honest take

If someone uses Apple devices and does not want to think too much about browser choices, Safari is a good answer. It is not the most customizable, but it is simple and safe enough for many people.

4. Google Chrome - strong security, not my favorite for privacy

Chrome is strong when it comes to security and website compatibility. It warns about dangerous sites and downloads, and many websites are built with Chrome in mind.

- Strong protection against known dangerous websites and downloads.
- Very good compatibility with most websites.
- Frequent security updates.
- Privacy is more complicated because Chrome is part of the Google ecosystem.

My honest take

Chrome is safe and convenient. Chrome is not my first privacy pick. Security and privacy are related, but they are not the same thing.

EDGE AND DUCKDUCKGO

5. Microsoft Edge - best built-in choice for Windows users

Microsoft Edge is much better than Internet Explorer ever was, which is not exactly a high bar, but still, credit where credit is due.

- Built into Windows.
- Works well with Microsoft accounts and Windows security.
- Microsoft Defender SmartScreen helps block phishing, malware sites, and risky downloads.
- Acceptable and safe enough for normal everyday use.

My honest take

Edge is not a bad browser. Weird sentence to write, but here we are. For Windows users, Edge is acceptable. I still prefer Brave or Firefox for privacy.

6. DuckDuckGo Browser - best simple privacy browser

DuckDuckGo is known for private search, but it also offers browsers and privacy protections. Its biggest strength is simplicity.

- Good for people who want less tracking.
- Helpful on phones.
- Simple privacy protection without a complicated setup.
- A privacy tool people actually use is better than a perfect tool they delete after ten minutes.

My honest take

DuckDuckGo Browser is a good simple choice. It may not be as powerful as Brave or Firefox for advanced users, but it is easy to understand. That matters.

TOR AND MULLVAD

7. Tor Browser - best for serious anonymity, not normal daily browsing

Tor Browser is built for privacy and anonymity. It can help protect users against tracking, surveillance, and censorship, but it is not the browser I would recommend for normal daily browsing.

- Routes traffic through the Tor network.
- Helps make users harder to track and fingerprint.
- Can be slower than normal browsers.
- Some websites block it or make logins annoying.
- Powerful, but not beginner-friendly for everyday use.

My honest take

Do not recommend Tor as the default browser for everyday users. That would be like giving someone a tank to drive to ShopRite. Technically protective, yes. Practical, no.

8. Mullvad Browser - best advanced privacy browser without using Tor

Mullvad Browser is a privacy-focused browser developed with the Tor Project. It is designed to reduce tracking and fingerprinting, especially for users who understand VPNs and privacy trade-offs.

- Strong focus on reducing fingerprinting.
- Can be used with or without a VPN.
- Better for advanced privacy users than beginners.
- For most people, I would start with Brave or Firefox first.

PRACTICAL RANKINGS

These are practical rankings for regular people, not a holy war in browser form.

Best overall for everyday people

1. Brave
2. Firefox
3. Safari
4. DuckDuckGo Browser
5. Edge
6. Chrome
7. Mullvad Browser
8. Tor Browser

Best for privacy

1. Tor Browser
2. Mullvad Browser
3. Brave
4. Firefox
5. DuckDuckGo Browser
6. Safari
7. Edge
8. Chrome

Best for beginners

1. Safari, for Apple users
2. Brave
3. DuckDuckGo Browser
4. Edge, for Windows users
5. Firefox

Why the rankings differ

The best browser depends on the goal. Best for privacy is not always best for beginners. Best for compatibility is not always best for privacy. The real question is: safe from what?

PRIVACY VS SECURITY

This is important

Privacy and security are related, but they are not the same thing. That is why "what is the safest browser?" is not always one answer.

Topic	Plain-English meaning	Examples
Security	The browser helps protect you from danger.	Fake websites, malware, dangerous downloads, phishing pages, suspicious extensions, scam pop-ups.
Privacy	The browser helps reduce how much you are tracked.	Ad tracking, cookie tracking, cross-site tracking, fingerprinting, search tracking, data profiling.

Simple way to think about it

- Chrome is strong on security.
- Brave is strong on privacy and security.
- Firefox is strong on privacy.
- Safari is strong for Apple users.
- Tor is strongest for anonymity.

The real question

Safe from what? Safe from scams? Safe from malware? Safe from tracking? Safe from someone seeing your activity on the same device? The answer changes depending on the risk.

IMPORTANT BROWSER SETTINGS TO CHECK

Turn on stronger tracking protection

- Look for words like Tracking Prevention, Enhanced Tracking Protection, Shields, Privacy Protection, Block third-party cookies, or Prevent cross-site tracking.
- Turn these protections on when available.

Turn on phishing and malware protection

- Look for Safe Browsing, Enhanced Protection, SmartScreen, Fraudulent Website Warning, or Warn About Dangerous Sites.
- Do not turn these warnings off because some random website tells you to. A real website does not need you to weaken your browser to visit it.

Keep the browser updated

- Browser updates often fix security holes.
- Update the browser, phone, and computer.
- Annoying? Yes. Important? Also yes.

Be careful with browser extensions

- Only install extensions you actually need.
- Be careful with extensions that can read and change all data on websites, access browsing history, access the clipboard, manage downloads, or change search settings.
- That does not always mean the extension is bad, but it means you should slow down and ask why it needs that much control.

THE BROWSER IS ONLY ONE PART

Use a password manager

- Use a password manager or trusted built-in password tools from Apple, Google, Microsoft, or another provider you trust.
- A good browser plus bad passwords is still a problem.
- Because apparently "Summer2024!" still refuses to retire.

Turn on two-factor authentication

- Use two-factor authentication for email, banking, credit cards, social media, Apple, Google, Microsoft, and your password manager.
- The browser helps protect the road. Two-factor helps protect the door. You need both.

Use fewer extensions

- More extensions can mean more tracking, more risk, and more things to manage.
- If you do not use it, remove it.
- Extensions are useful until your browser turns into a junk drawer with Wi-Fi.

Simple habit check

Trusted browser. Strong passwords. Two-factor authentication. Updated devices. Fewer extensions. Less panic. More thinking before clicking.

WHAT PRIVATE BROWSING REALLY MEANS

Private does not mean invisible

Private browsing usually means the browser does not save certain activity on that device. It does not automatically hide everything from the entire internet. Because, of course, the word private had to come with fine print. Very helpful.

Private browsing usually does not save

- Browsing history from that private session.
- Search history from that private session.
- Cookies from that private session.
- Some form information.

Private browsing may still be visible to

- Your internet provider.
- Your employer or school network.
- Websites you visit.
- Apps or accounts you log into.
- Public Wi-Fi owners.
- Some tracking systems.

Plain-English translation

Read private browsing as private from other people using the same device, not private from the entire internet.

WHAT I WOULD TELL AN EVERYDAY USER

Simple browser advice

- Use Brave if you want the best all-around privacy and safety.
- Use Safari if you are deep in the Apple world and want something simple.
- Use Firefox if you want a good privacy browser from a well-known company.
- Use Chrome if you care most about security and website compatibility, but understand that it is not my top privacy choice.
- Use Edge if you are on Windows and want something built in that is safe enough.
- Use DuckDuckGo Browser if you want a simple private browser, especially on your phone.
- Use Tor only when anonymity really matters.
- Use Mullvad Browser if you are more advanced and want stronger fingerprinting protection without using Tor.

Final advice

The browser matters, but your habits matter more. A safe browser helps. Strong passwords help. Two-factor authentication helps. Updates help. Not clicking every strange link helps even more.

The real goal

Regular people do not need to become computer experts. They need simple habits that make them harder targets.

SOURCE NOTES

Information checked against official browser and company sources on June 21, 2026. Features and menu names can change, because apparently software likes to move the furniture while we are not looking.

Sources checked

Source	What was checked
Brave	Privacy Features and Brave Shields pages for tracker blocking, cross-site cookie blocking, and fingerprinting protections.
Mozilla Firefox	Total Cookie Protection and Enhanced Tracking Protection support pages.
Apple Safari	Safari privacy features, Privacy Report, Intelligent Tracking Prevention, and Safari privacy documentation.
Google Chrome	Google Safe Browsing and Chrome safety pages for phishing, malware, and dangerous download warnings.
Microsoft Edge	Microsoft Defender SmartScreen support pages for phishing, malware, and risky download protections.
Tor Browser	Tor Project pages for tracking, surveillance, censorship, and fingerprinting protections.
DuckDuckGo	DuckDuckGo browser and web tracking protection pages.
Mullvad Browser	Mullvad Browser and Tor Project launch information on reducing tracking and fingerprints.

Use this responsibly

Browser recommendations are practical guidance for everyday users. They are not a guarantee, not legal advice, and not a magic shield against every scam. The safest setup is a trusted browser plus better habits.

SECURE MESSAGING APPS FOR IPHONE AND ANDROID

A plain-English guide to private texting and calling

What secure messaging means

Secure messaging apps help protect private conversations by using end-to-end encryption. In plain English, that means the message is locked on the sender's phone and unlocked on the receiver's phone. The app company should not be able to read the actual message while it is being sent. Signal, WhatsApp, iMessage, and Google Messages all offer end-to-end encryption in certain situations.

What secure messaging does not fix

A secure messaging app is helpful, but it is not magic. If someone steals your phone, guesses your passcode, sees your notifications, or tricks you into sharing a login code, the app cannot fully protect you. The best habit is to use a trusted secure messaging app, keep your phone locked, update your apps, and never share passwords or verification codes through text.

Secure Messaging Apps I Recommend

App	iPhone	Android	Best for	My take
Signal	Yes	Yes	Best overall	Best balance of security, privacy, and normal-person usability.
SimpleX Chat	Yes	Yes	Maximum privacy	No phone numbers, no usernames, no user IDs. Strong privacy, but less familiar.
Threema	Yes	Yes	Private paid messaging	No phone number or email required. No ads, no tracking, no profiling.
Session	Yes	Yes	No phone number	Privacy-focused messaging without a phone number or email. Less mainstream.
Element	Yes	Yes	Groups and communities	Built on Matrix. Better for groups and self-hosting than casual family texting.
Wire	Yes	Yes	Professional use	Work-focused secure messaging. Good, but not my first pick for everyday family use.

For most people, Signal is one of the strongest choices for private texting and calling because it is built around privacy and says it cannot read your messages or listen to your calls. WhatsApp is also widely used and protects personal chats with end-to-end encryption, which makes it easier for families and friends because many people already have it.

On iPhone, iMessage is protected when you are messaging another Apple user. On Android, Google Messages can protect RCS chats when everyone in the conversation is using Google Messages with RCS turned on. Not every text message is automatically protected the same way, so that part matters.

My opinion

1. Signal, best overall

Signal is the one I would recommend first because it is easy to use, end-to-end encrypted, not owned by Meta, and designed to collect as little sensitive information as possible. Signal also supports usernames and phone-number privacy, which helps fix one of the old complaints about needing to expose your phone number to everyone.

Best for: family, friends, business conversations, and private everyday messaging.

Downside: you still need a phone number to register.

2. SimpleX Chat, best for privacy

SimpleX is probably the strongest privacy pick on this list because it says it has no user IDs, not even random ones. That is a big deal because most apps still identify you somehow, even if they encrypt the messages.

Best for: people who want serious privacy and do not want phone numbers or usernames tied to chats.

Downside: less common, so getting other people to use it may be the usual “please install another app” circus.

3. Threema, best paid private app

Threema does not require a phone number or email address, uses end-to-end encryption, and says it has no advertising, tracking, or profiling. That is exactly the kind of sentence I like seeing from a messaging app.

Best for: people who want a clean, private, non-Meta app and do not mind paying.

Downside: fewer people use it, and the paid model may stop some people from joining.

Quick reminder

A secure app only protects the message path. It cannot protect you from a weak phone passcode, message previews on the lock screen, a compromised phone, or giving a scammer your login code.

4. Session, best no-phone-number option

Session does not require a phone number or email to sign up. It also focuses heavily on metadata protection, which means it tries to protect not just what you say, but also the surrounding information about your communication.

Best for: privacy-focused users who do not want to register with personal information.

Downside: it is less mainstream, and I would treat it as better for messaging than for the most sensitive voice calling situations.

5. Element, best for groups and communities

Element is based on Matrix and supports end-to-end encrypted messaging and calls. It is a good choice for groups, communities, and organizations that want more control, especially if they care about decentralization or self-hosting.

Best for: teams, communities, private groups, or organizations.

Downside: more complicated than Signal for everyday people.

6. Wire, best for professional use

Wire is end-to-end encrypted and aimed more at organizations, teams, and professional communication. It can work personally, but I would not put it ahead of Signal, SimpleX, or Threema for normal day-to-day secure messaging.

Best for: business, teams, professional conversations.

Downside: not the easiest recommendation for regular family and friend texting.

Apps That Deserve Extra Consideration

App	Things to consider
WhatsApp	End-to-end encrypted, but owned by Meta. Some privacy-conscious users prefer alternatives because of metadata collection concerns.
Facebook Messenger	Convenient, but not my recommendation for sensitive conversations.
Instagram DMs	Fine for casual social communication, not my first choice for private discussions.
Telegram	Secret Chats offer end-to-end encryption, but regular chats do not use it by default.
SMS / Text Messages	Not end-to-end encrypted and should not be considered private.

My personal recommendation

Best overall: Signal, easy to use

Best privacy-first option: SimpleX Chat

Best no-phone-number paid option: Threema

Best anonymous-style messaging option: Session

Best group or community option: Element

My final answer

Tell most people to use Signal. Tell privacy-focused people to look at Session, SimpleX, or Threema.

Simple habits that matter

- Turn on your phone passcode or biometric lock.
- Keep message previews off on the lock screen if privacy matters.
- Update your phone and your messaging apps.
- Do not share one-time verification codes over text.
- Be careful with backup settings, cloud sync, and linked devices.
- Remember that the other person's phone security matters too.

Security is not only about the app. It is also about the habits around the app. A private messenger on an unlocked phone is still a problem, because of course it is.

Source note: Feature descriptions were checked against official sources from Signal, WhatsApp, Apple, Google Messages, SimpleX Chat, Threema, Session, Element, and Wire. Features can change over time.

HIDDEN APPS AND DELETED APP CLUES

A parent-friendly checklist for iPhone and Android

Who this handout is for

This handout is for parents and caregivers checking a family-owned device, a child's device they manage, or their own phone. Start with a conversation when possible. Do not break into accounts, guess passwords, bypass locks, or secretly access someone else's private information.

Important reminder

A hidden app is a clue, not a conviction. Some privacy apps are normal. Look at the full picture: behavior changes, unsafe contacts, scams, bullying, threats, or content that puts someone at risk.

What hidden or vault apps may look like

May look like	What it may do
Calculator or fake calculator	May hide photos, videos, files, notes, passwords, or chats behind a PIN.
Gallery, photo manager, or file manager	May store private media or folders under a normal-looking icon.
Notes, calendar, clock, audio player, or utilities	May be a decoy screen with a vault underneath.
Security tool, app locker, or clone tool	May lock apps, hide apps, clone apps, or create a second login space.

Names change often, so do not rely on one app-name list. Look for patterns instead: boring names, duplicate icons, large storage use, and permissions that do not make sense.

Examples of names parents may see

Platform	Example names
iPhone examples	Private Photo Vault, Keep Safe, Secret Photo Album, Locker, Note Lock, iVault, HiddenVault, Secret Calculator Vault
Android examples	Calculator+, Vault-Hide, GalleryVault, App Hider, Dialer Vault, Calculator Lock, Hide It Pro, Clock Vault, Notepad Vault

Do not panic over the name alone

The better question is this: does the app activity match what the person says they are using the phone for? If not, slow down and ask questions.

IPHONE CHECKLIST

Places parents can check together

1. Check hidden apps

- Check the App Library and look for the Hidden folder. It may require Face ID, Touch ID, or the passcode.
- On newer iPhones, check Settings > Apps > Hidden Apps.
- Apple says hidden app names may still appear in Screen Time, Battery Usage by App, and App Store purchase history.

2. Check Screen Time and Battery

- Settings > Screen Time > See All App & Website Activity
- Settings > Battery > Battery Usage by App
- If a boring-looking app is used constantly, write it down and ask about it. Do not treat it as proof by itself.

3. Check App Store history

- Open the App Store, tap the profile photo, then check Purchase History.
- Also check Purchased or My Purchases if Family Sharing is used.
- Deleted apps may no longer show on the Home Screen, but download history may still show them.

4. Check photos and recently deleted content

- Photos > Albums or Collections > Utilities > Hidden
- Photos > Albums or Collections > Utilities > Recently Deleted
- Settings > Apps > Photos > Show Hidden Album, this setting may hide or show the Hidden album.

5. Search and browser clues

- Search words like vault, hide, private, secret, locker, calculator, photo, folder, and browser.
- Look inside folders with boring names like Utilities, Tools, School, Notes, or Extras.
- An empty browser history does not prove anything. It may mean private browsing, cleared history, restrictions, or normal cleanup.

ANDROID CHECKLIST

Menus change by brand, but the clues are similar

1. See all installed apps

- Settings > Apps > See all apps
- Look for duplicates, strange names, apps with blank icons, and apps that do not match their claimed purpose.

2. Check app permissions

- Settings > Security & privacy > Privacy > Permission manager
- Review camera, microphone, files, photos, contacts, location, and SMS access.
- A calculator app asking for photos, camera, microphone, contacts, or SMS access deserves a closer look.

3. Check storage and battery

- Settings > Storage > Apps
- Settings > Battery, then look for app battery usage.
- If a simple app is using hundreds of megabytes or gigabytes, it may be storing media or files.

4. Check deleted or previously installed apps

- Open Google Play Store, tap the profile icon, then Manage apps & device.
- Go to Manage, then filter for Not installed if available.
- This can show apps that were downloaded before but are not currently installed.

5. Check private spaces

- Android Private Space may appear under Settings > Security & privacy > Private space.
- Samsung Secure Folder may appear under Settings > Security and privacy > More security settings > Secure Folder.
- These features can hold apps and files behind another lock. Do not try to bypass the lock. Talk first, especially with a teenager.

6. Check files and folders

- Use Files by Google or the phone's built-in file manager.
- Check Downloads, Pictures, Movies, Documents, and folders with random names.
- Do not delete anything important until you understand what it is.

DELETED APP AND HISTORY CLUES

What to check without turning this into a spy movie

iPhone clues

- App Store download or purchase history may show apps that are not currently on the Home Screen.
- Hidden and Recently Deleted albums can show photo activity that is not obvious in the main photo view.
- Screen Time and Battery can show activity from apps with boring names.
- iCloud backup settings may show apps connected to backups, depending on how the device is set up.

Android clues

- Google Play > Manage apps & device > Manage > Not installed can show apps downloaded before.
- Files by Google or another file manager may show unusual folders.
- Google account activity should only be checked for your own account or a child account you legally manage.
- Samsung Secure Folder can exist even when the icon is hidden from the home screen.

Privacy and trust matter

Checking a phone secretly can damage trust fast. If the child is in danger, safety comes first. If this is a family safety check, do it together when possible and explain what you are looking for.

What counts as a real concern?

One hidden app is not automatically a crisis. Bigger concerns include unsafe contacts, threats, blackmail, bullying, sexual content involving a minor, scams, self-harm concerns, or major behavior changes.

5-MINUTE FAMILY CHECK

Use this as a simple checklist

Check these items together

- ☐ Duplicate apps, like two calculators, two galleries, or two browsers
- ☐ App names that sound boring but have heavy use
- ☐ App permissions that do not match the app
- ☐ App storage size
- ☐ Battery usage
- ☐ Screen Time on iPhone or Digital Wellbeing on Android
- ☐ Hidden and Recently Deleted photos
- ☐ App Store or Google Play download history
- ☐ Private browsers
- ☐ Android Private Space or Samsung Secure Folder
- ☐ Google account activity, only for your own account or a child account you legally manage
- ☐ Cloud backup settings and shared devices

What to do if something feels wrong

- Stay calm. A calm parent gets more information than a screaming parent. Shocking, I know.
- Ask direct questions: What is this app for? Who showed it to you? Is anyone pressuring you?
- If there are threats, bullying, blackmail, sexual content involving a minor, or safety concerns, save evidence and get help from the school, a counselor, or law enforcement.
- Use parental controls where appropriate, but do not make the whole relationship about catching them. That usually teaches better hiding, not better safety.

Final reminder

The goal is not to win an argument over a phone. The goal is to keep the person safe, help them understand risk, and make sure they know they can come to you before a mistake becomes a disaster.

WEBSITE AND ACCOUNT ORGANIZER

A simple worksheet for organizing login details safely

Purpose

Use this document to organize your own personal list of website and app login details. Set it up in a way that feels comfortable and makes sense to you. Copy one blank block per site and keep everything consistent.

How to use this document

- For each website or app, copy one blank template block and paste it below.
- Enter the website or app name exactly as it appears on your phone or computer.
- Paste the full HTTPS link so the correct site opens every time.
- Use the same ID format for all accounts, usually an email address.
- If you choose to store a password here, make it long and unique. Aim for at least 15 characters.
- Only fill in security questions if the site actually uses them.
- Use the Notes section for anything helpful later, like 2FA method, backup codes location, account owner, or reminders.

Basic safety rules

- Do not email this document.
- Do not store it in a shared folder.
- If passwords are included, store this file in a password-protected or encrypted location.
- If you use a password manager, replace PW with the password manager entry name.

Quick note

This document is an organizer, not a safe. Treat it like cash. Store it somewhere private and non-obvious. Do not store real passwords in this document unless the file is kept in a password-protected or encrypted location. A safer option is to write the password manager entry name instead of the actual password. For organization, keep your list in alphabetical order. Please do not name the folder Trash or Garbage. That is the first place someone would look.

SAMPLE PAGE

Example only. Do not use these as real login details.

Website and Account Organizer

Last reviewed: ____ / ____ / ____

Update this date every time you add or change anything.

Apple

<https://www.apple.com>

ID: example@email.com

PW: Password manager entry

2FA: On, authenticator app

Notes: Apple ID, recovery email confirmed

Best Buy

<https://www.bestbuy.com>

ID: example@email.com

PW: Password manager entry

2FA: On, text message

Notes: Receipts sent to this email

BJ's

<https://www.bjs.com>

ID: example@email.com

PW: Password manager entry

2FA: On

Notes: Membership tied to this account

Bed Bath and Beyond

<https://www.bedbathandbeyond.com>

ID: example@email.com

PW: Password manager entry

2FA: Off, review settings

Notes: Membership tied to this account

BLANK ACCOUNT BLOCKS

Copy one block per website or app. Keep the list in alphabetical order.

Blank templates

Website or app name: _____
Full HTTPS link: _____
ID or username: _____
PW or password manager entry: _____
2FA method: _____
Notes: _____

Website or app name: _____
Full HTTPS link: _____
ID or username: _____
PW or password manager entry: _____
2FA method: _____
Notes: _____

Website or app name: _____
Full HTTPS link: _____
ID or username: _____
PW or password manager entry: _____
2FA method: _____
Notes: _____

Website or app name: _____
Full HTTPS link: _____
ID or username: _____
PW or password manager entry: _____
2FA method: _____
Notes: _____

MORE BLANK ACCOUNT BLOCKS

Use these if you are printing the organizer.

Blank templates

Website or app name: _____

Full HTTPS link: _____

ID or username: _____

PW or password manager entry: _____

2FA method: _____

Notes: _____

Website or app name: _____

Full HTTPS link: _____

ID or username: _____

PW or password manager entry: _____

2FA method: _____

Notes: _____

Website or app name: _____

Full HTTPS link: _____

ID or username: _____

PW or password manager entry: _____

2FA method: _____

Notes: _____

Website or app name: _____

Full HTTPS link: _____

ID or username: _____

PW or password manager entry: _____

2FA method: _____

Notes: _____

