Digital Home Security & Privacy

Todd Luttmers | Senior Financial Advisor | Keystone Private Wealth

Primary Reference: privacyguides.org

Who Is This Guy?

Then

Now

Same kid. Better tools.

The Finance Side

- Senior Financial Advisor
- Keystone Private Wealth
- Protecting client data is my #1 priority

The Tech Side

- Tech enthusiast since childhood
- Built PCs, run my own home server
- Not here to sell — just sharing what I know

Section 1

Privacy vs. Security What's the difference?

Privacy vs. Security: Not the Same Thing...

🔍 Privacy

Controlling who sees your information

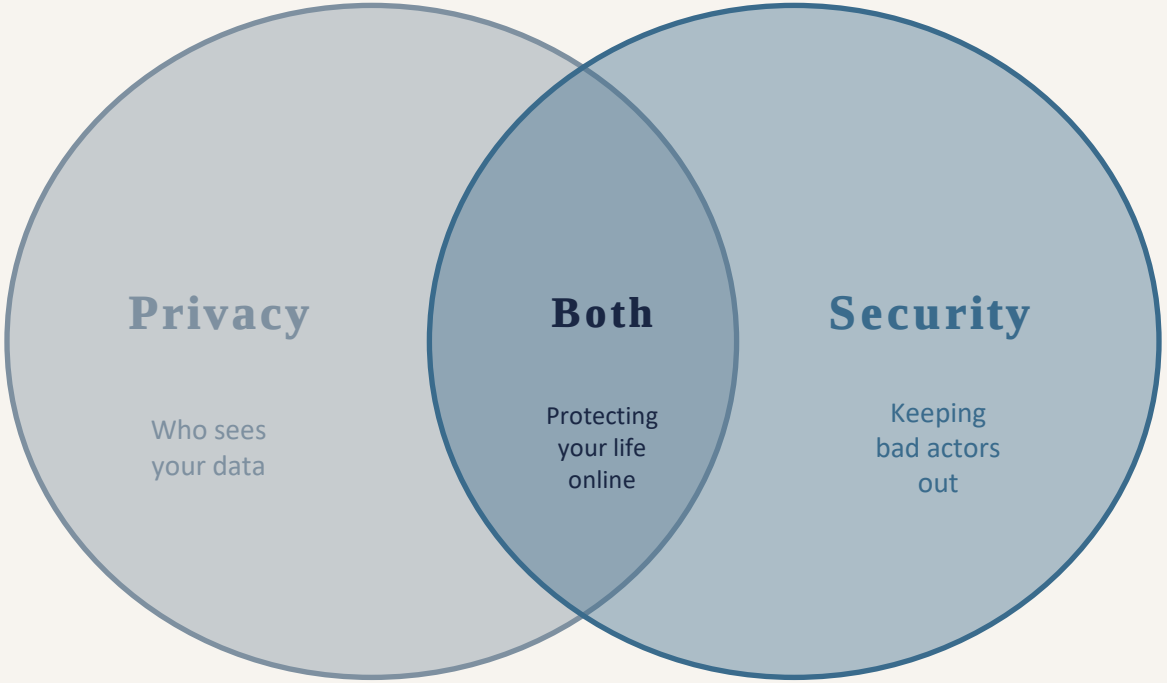
- Your doctor knows your health history — that's private
- Your neighbor does NOT need to know — that's a privacy issue
- Privacy = who has access to your data
- Example: Posting your home address on Facebook

🔒 Security

Protecting your data from being stolen

- A locked safe protects what's inside it
- If a thief breaks in, your security failed
- Security = preventing unauthorized access
- Example: Someone guessing your email password

How They Work Together



The Bottom Line

- Good security helps protect your privacy
- But security alone doesn't guarantee privacy
- You need BOTH to stay truly safe online

Section 2

Why You Should Care

Real Stories. Real Consequences.

Spoiler: 'I have nothing to hide' is not a defense strategy.

Why Privacy Matters

Privacy isn't about hiding secrets — it's about power.

> *"We know what happens in the bathroom, but you still close the door. That's because you want privacy, not secrecy."*

Privacy Is Power

Your information confers power over you. Whoever holds your data — your habits, health, finances, location — holds leverage over your life. Privacy determines who has that power.

"Nothing to Hide" Is a Trap

Saying you don't need privacy because you have nothing to hide is like saying you don't need free speech because you have nothing to say. Rights exist for when you need them.

You're the Product

Meta made $165B and Google $350B in 2024 — almost entirely from selling access to YOUR attention, shaped by YOUR data. If you're not paying, you're what's being sold.

Control Is an Illusion

Cookie banners and privacy dashboards make you feel in control. In reality, they're designed to make you click "I Agree." Real privacy must be built into the tools you use.

Privacy ≠ Secrecy

You're not hiding crimes. You're protecting your medical records, your finances, your family photos, your location. These are normal things that deserve protection.

It's Yours to Protect

Privacy isn't a lost cause. Every setting you change, every app you remove, every password you strengthen takes back a piece of control. Small actions compound.

Source: privacyguides.org | Video: "Privacy is Power. And You're Giving Yours Away." (2025)

Data Brokers: The Business of YOU

$240B+

Annual data broker industry revenue

💡 *Tip: Search your name on Spokeo.com to see what they have on you. You'll be surprised.*

Who are data brokers?

- Companies that collect, buy, and sell YOUR personal information — without your knowledge
- They know your name, address, phone, income, health history, buying habits, and more
- Anyone can BUY a profile on you for just a few dollars
- Examples: Acxiom, LexisNexis, Spokeo, BeenVerified, Whitepages
- Scammers and identity thieves use these services too

"Smart" Home Devices Aren't Always Smart About Privacy

⚠️ The Roomba Incident: When Your Vacuum Becomes a Paparazzi

In 2022, images captured by iRobot Roomba vacuum cleaners — including photos of a woman in the bathroom — were leaked online after being shared with data annotators via a third-party vendor. The images were never meant to leave the home. This is the world we live in.

Other devices listening and watching in your home:

- Smart TVs: Many record voice commands and viewing habits and sell the data to advertisers
- Smart speakers (Alexa, Google Home): Always listening for a wake word — and sometimes accidentally recording private conversations
- Smart doorbells & cameras: Video footage can be accessed by companies and, in some cases, shared with law enforcement without your knowledge

Meta Smart Glasses: You're Being Watched (Literally)

How It Works

- Meta Ray-Ban smart glasses have a built-in camera — and it's almost invisible
- Two Harvard students demonstrated they could identify a stranger's face in real time, find their home address, and approach them by name — all in seconds
- The only indicator? A tiny LED light that can be taped over
- Combined with AI face recognition, anyone wearing these glasses can look up who you are just by looking at you

😬 The Scary Part

The person sitting across from you at a coffee shop, a doctor's office, or a community event could identify you, find your home address, and know your financial history — all before you finish your coffee.

Source: Harvard students' I-XRAY project, October 2024

"Real-Time Pricing" — Paying More Because of Who You Are

Dynamic pricing uses your data — location, browsing history, loyalty program status, even what device you use — to charge YOU a different price than your neighbor for the exact same item.

Real Examples That Affect You:

🏬 Macy's

Macy's has piloted dynamic pricing where identical items show different prices based on your loyalty tier, browsing history, and device.

✈️ Airlines & Hotels

Airlines and hotel booking sites have been known to show higher prices to users who searched the same route multiple times — use Incognito mode to compare.

🛒 Grocery Stores

Digital shelf labels can change prices multiple times per day. Kroger and others have tested surge pricing during peak hours — like Uber, but for milk.

AI Is Reading Your Emails. No, Really.

What Google Does With Your Gmail:

- Gmail scans the content of your emails to personalize ads — your emails are processed by automated systems
- Google's AI reads flight confirmations, order receipts, and bank statements to populate Google Assistant
- In 2018, Google admitted third-party app developers could also read user emails — not just Google's own systems
- Microsoft Outlook, Yahoo Mail, and others have similar data practices

🔒 Better Alternatives

- ProtonMail — end-to-end encrypted, based in Switzerland
- Tutanota — free encrypted email alternative
- Both recommended by privacyguides.org

Don't have to switch — but know what you're giving up.

A Friend Got Hacked — Here's How They Did It

The Anecdote

A friend of mine received a convincing phone call from someone posing as his mobile carrier. The caller said there was 'suspicious activity' on his account and they needed to verify his identity. The caller read back his personal information — his address, last 4 digits of his SSN, recent calls. It sounded completely legitimate. Within minutes, his phone number was transferred to the attacker's SIM card. His bank's text message security codes went straight to the hacker.

What is SIM Swapping?

- Attackers convince your mobile carrier to transfer your phone number to their SIM card
- Once they have your number, they receive ALL your text message security codes (2FA)
- They can then reset passwords on your bank, email, investment accounts
- A SIM swap attack stole $400 million from crypto exchange FTX — charges were filed in 2024

How to Protect Yourself

- Set a SIM PIN or port freeze with your carrier
- Never give security codes to callers
- Use an authenticator APP instead of SMS for 2FA

Deepfakes: When Seeing Is No Longer Believing

AI can now generate fake videos and audio of ANYONE saying or doing ANYTHING — using just a few photos or a short voice clip from social media.

💸 Financial Fraud

A Hong Kong company lost $25 million in 2024 after an employee was tricked by a deepfake video call impersonating the CFO, who instructed the transfer of funds.

👨‍👩‍👧 Family Scams

"Grandparent scams" now use AI voice cloning. You receive a call that sounds EXACTLY like your grandchild saying they're in trouble and need money. Multiple seniors in Arizona were victimized in 2023.

🏛️ Political Manipulation

Fake audio of candidates saying things they never said, created just before elections. Deepfake robocalls impersonating President Biden were used in the 2024 New Hampshire primary.

🔑 *Key Rule: Establish a family "safe word" you can use to verify identity in emergencies.*

Section 3

Know Your Threats

Before you defend, you need to understand what you're defending against.

Think like a burglar to protect your house.

What Is a Threat Model?

A threat model is simply asking: Who wants my stuff, what do they want, and how would they get it?

Who?

Your adversaries

- Scammers & con artists
- Data brokers & advertisers
- Hackers (opportunistic)
- Nosy people / bad actors

What?

What they're after

- Your money & accounts
- Your identity (SSN, DOB)
- Your login credentials
- Your personal habits & data

How?

Their methods

- Phishing emails & texts
- Phone scams / social engineering
- Public Wi-Fi snooping
- Data breaches & leaks

Everyone has a different threat model. A retiree in Palm Desert has different risks than a 25-year-old in New York.

Threat Vectors: How Attackers Get In

A threat vector is a path an attacker uses to reach you. Here are the most common ones:

Phishing — 91%

Fake emails or texts pretending to be your bank, the IRS, or a company you trust. They want you to click a link or give up credentials.

Social Engineering — 68%

Phone calls from someone pretending to be tech support, your carrier, or a grandchild in trouble. They manipulate trust, not technology.

Public Wi-Fi — 25%

Coffee shop and hotel Wi-Fi lets attackers see your traffic. Logging into your bank on public Wi-Fi is like shouting your password.

Data Breaches — 83%

Companies you trusted get hacked. Your passwords, SSN, and financial info end up for sale on the dark web. You can't prevent these.

Unpatched Software — 57%

Old software has known security holes. Hackers scan for devices running outdated systems and walk right in.

Physical Access — 46%

Someone who gets your unlocked phone, your mail, or access to your computer can do more damage than any hacker.

91% = cyberattacks starting with phishing (Deloitte). 68% = human element in breaches (Verizon DBIR 2024). Other figures from IBM, CISA reports.

Section 4

What You Can Do About It

Good news: you don't have to be a tech wizard. Every step helps.

Reference: privacyguides.org

Level 1: Beginner — Start Here Today

01

Use Strong, Unique Passwords

Use a password manager like Bitwarden (free) or 1Password. Never reuse passwords. One breach = every account compromised.

02

Enable Two-Factor Authentication (Authenticator App)

Use Google Authenticator, Authy, or similar. NOT text/SMS. This prevents SIM swap attacks.

03

Update Your Software Regularly

Hackers exploit old, unpatched software. Enable automatic updates on your phone, computer, and router.

04

Check If You've Been Hacked

Visit haveibeenpwned.com — enter your email to see if it's in a known data breach. Free and takes 10 seconds.

🔑 Passwords: Your Digital Front Door Lock

🙋 Interactive Exercise

Turn to the person next to you and share your pet's name and your birth month. Congratulations — you may have just guessed each other's password.

59%

of US Adults use birthdays or names in their passwords

22% own name
33% pet's name
14% children's names
15% spouse / partner

✅ What Makes a Strong Password?

- 12+ characters minimum (longer = stronger)
- Mix of UPPERCASE, lowercase, numbers & symbols (!@#$)
- No dictionary words, names, or dates
- Unique password for every single account — never reuse!

❌ Weak Password	✅ Strong Password
Fluffy1985 *(cracked in under 1 second)*	*kP9#mR2!vX4@nQ7$* *(cracked in 34,000+ years)*

🔐 **Password Manager Recommendation: Bitwarden (free) or 1Password — generate & store strong unique passwords so you only remember ONE master password.**

🍎 iPhone Beginner Security — Lesson 1

Source: privacyguides.org

01

🗑️ Delete Unused Apps

Settings → General → iPhone Storage

Every app is a door. Fewer apps = smaller attack surface. If you haven't opened it in 3 months, delete it.

02

🔐 Use a Strong Passcode

Settings → Face ID & Passcode → Change Passcode → Custom Alphanumeric

Face ID alone can be compelled. A 6+ digit PIN or alphanumeric code is much harder to crack.

03

📍 Limit Location Access

Settings → Privacy & Security → Location Services

Set most apps to "While Using" or "Never." Few apps actually need your location all the time.

04

🚫 Turn Off App Tracking

Settings → Privacy & Security → Tracking → toggle OFF

This single toggle stops hundreds of ad networks from following you across every app you open.

05

Enable Automatic Updates + Turn Off Analytics Sharing

Settings → General → Software Update → Automatic Updates ON

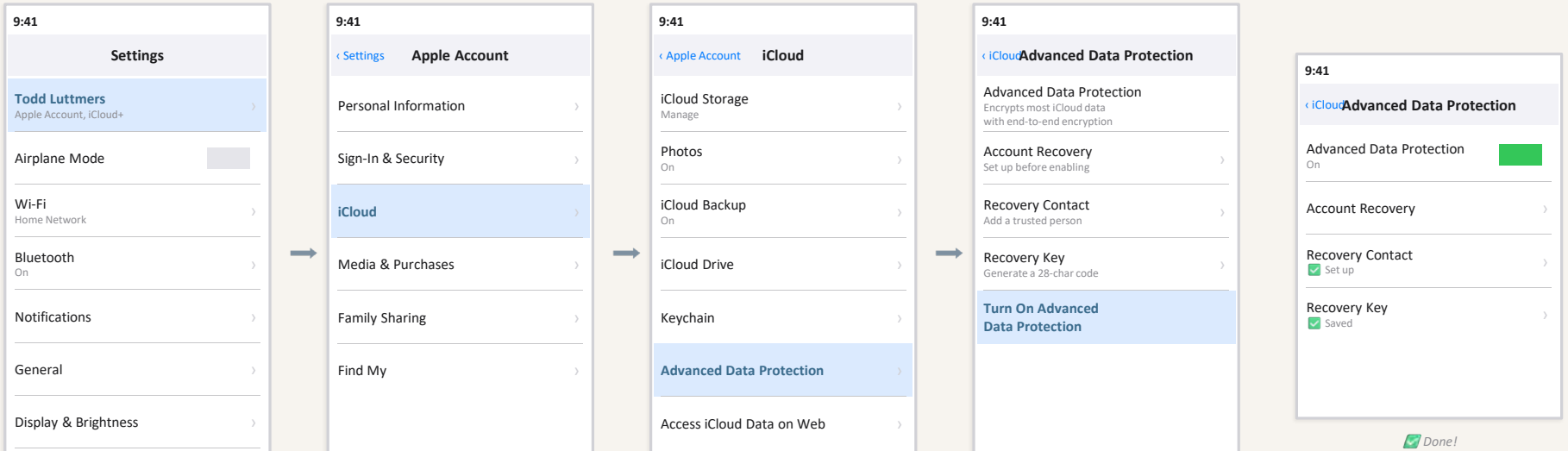
Settings → Privacy & Security → Analytics & Improvements → toggle ALL off

⚠️ *Reference the 2025 Apple Siri $95M settlement — Siri was recording private conversations including medical appointments and business calls.*

Source: privacyguides.org Smartphone Security Course Lesson 1

Step 1: Enable Advanced Data Protection

End-to-end encrypts your iCloud backups, photos, notes & more — even Apple can't read your data.



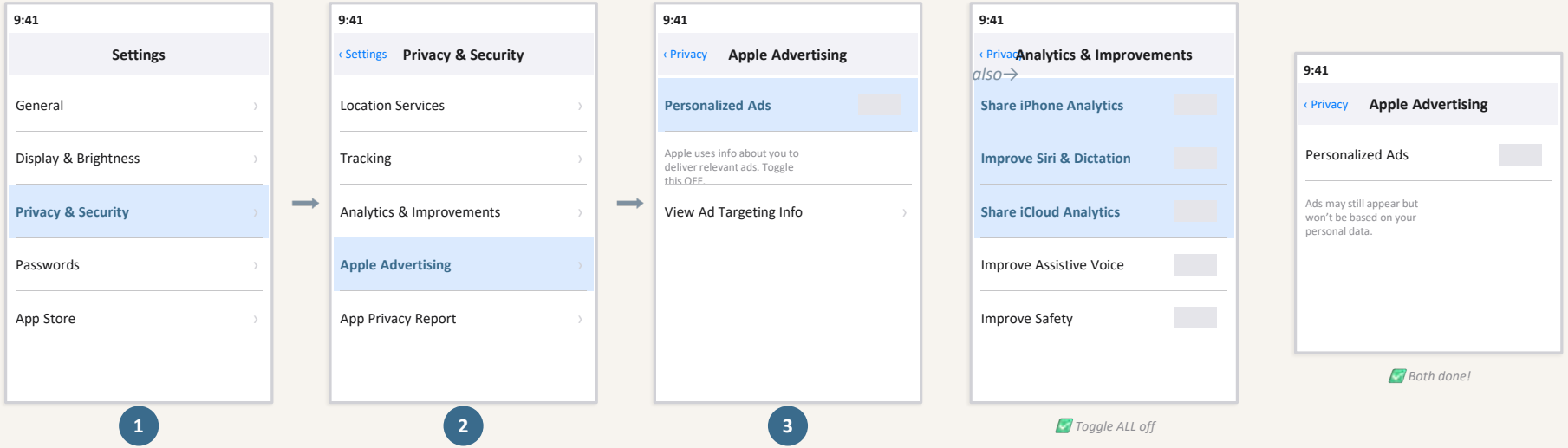
⚠️ **Important:** You'll be asked to set up a Recovery Contact or Recovery Key first. This is required because once enabled, Apple cannot help you recover data — only you hold the keys. Follow the on-screen prompts.

Requires iOS 16.2 or later | Source: support.apple.com/en-us/108756

Step 2: Turn Off Personalized Ads & Analytics

Two places to change — Apple Advertising and Analytics & Improvements.

Path A: Apple Advertising



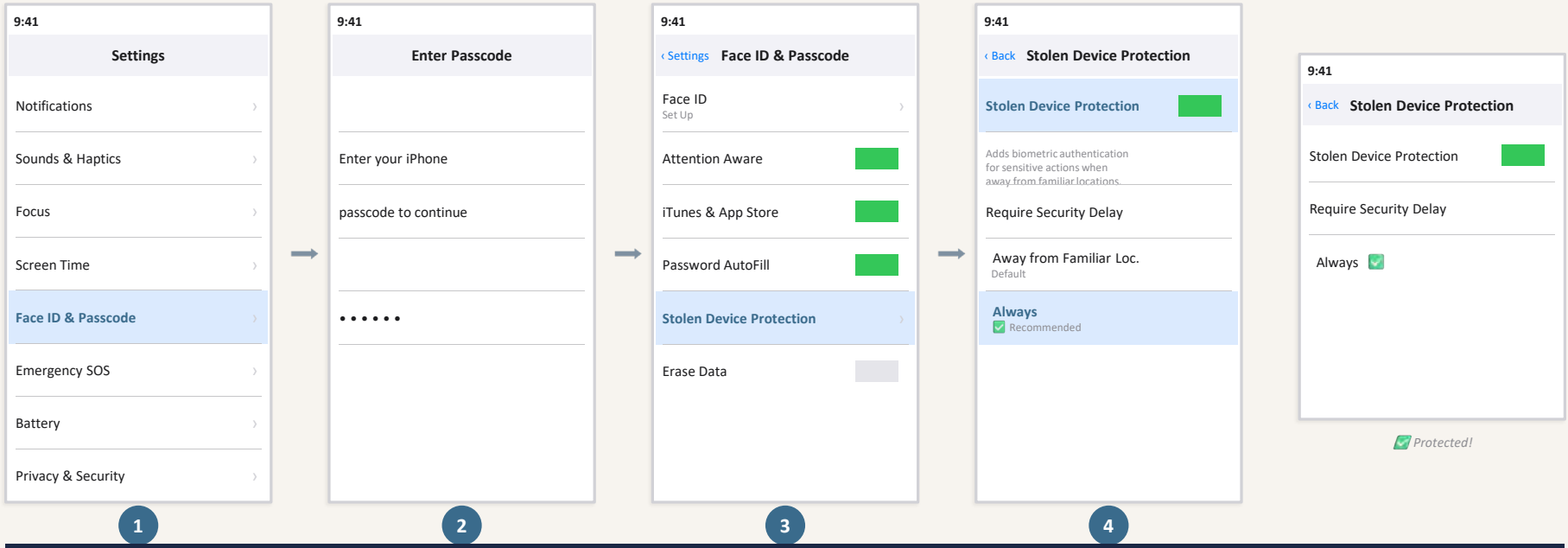
Path B: Analytics & Improvements

This stops Apple from using your data for targeted ads AND stops sharing your usage analytics. Two taps, two huge privacy wins.

Reference: 2025 Apple Siri $95M settlement — Siri was recording private conversations. These analytics toggles control what Apple collects.

Step 3: Turn On Stolen Device Protection

If a thief steals your phone AND knows your passcode, this blocks them from taking over your life.



What this blocks: Even with your passcode, a thief CANNOT change your Apple ID password, turn off Find My, access saved passwords, use saved credit cards, or erase your device — without your face or fingerprint. Set to "Always" for maximum protection.

Requires iOS 17.3+ | Face ID or Touch ID + Find My must be enabled | Source: support.apple.com/en-us/120340

Android Beginner Security — Lesson 1

Source: privacyguides.org | Best hardware: Google Pixel

01

Delete Unused Apps

Settings → Apps → [App Name] → Uninstall

Each unused app is an open window. Removing them shrinks your 'attack surface' — fewer ways in for hackers.

02

Use a Strong PIN or Password

Settings → Security → Screen Lock → PIN or Password

Fingerprint alone can be defeated physically. A 6+ digit PIN is your legal and security backup.

03

Delete Your Advertising ID

Settings → Privacy → Ads → Delete Advertising ID

Google uses this ID to track everything you do across all apps. Deleting it is free and takes 5 seconds.

04

Audit App Permissions

Settings → Privacy → Permission Manager

See which apps can access your camera, microphone, location. Revoke anything that doesn't make sense.

privacyguides.org recommends the Google Pixel — 7 years of security updates vs. 2–3 years on most Android phones.

An unpatched Android phone is one of the highest-risk devices you can own. The Pixel 9 series receives updates through 2031.

Source: privacyguides.org Smartphone Security Course Lesson 1 (Android)

Level 2: Intermediate — Level Up Your Protection

01

Switch to a Private Browser

Use Firefox or Brave instead of Chrome. These don't build advertising profiles on you. Recommended by privacyguides.org.

02

Use a Private Search Engine

Try DuckDuckGo or Startpage instead of Google. Google logs every search you make and uses it to build your profile.

03

Use a VPN on Public Wi-Fi

A VPN encrypts your internet traffic. Critical when using coffee shop or hotel Wi-Fi. Recommended: Mullvad or ProtonVPN.

04

Opt Out of Data Brokers

Manually opt out of Spokeo, Whitepages, and others — or use a service like DeleteMe ($129/yr) to automate it.

Level 3: Advanced — For the Seriously Committed

(Todd-level stuff — but great to know it exists)

🔐 Use an Encrypted Email Provider

ProtonMail or Tutanota. Your emails are encrypted end-to-end — even the provider can't read them. Based outside US jurisdiction.

📵 De-Google Your Phone

GrapheneOS (for Pixel phones) removes Google's tracking from Android entirely. Not for the faint of heart, but it exists and works.

🌐 Use a Pi-hole at Home

A Raspberry Pi device that blocks ads and trackers at the network level — before they even reach your devices. Great for smart TVs too.

🗂️ Self-Host Your Data

Store your own files, photos, and passwords on your own hardware using tools like Nextcloud. Nothing goes to Google or Amazon.

🔑 Use Hardware Security Keys

A physical USB key (like YubiKey) that must be inserted to log in. Impossible to phish remotely.

📋 Compartmentalize Your Digital Life

Separate browsers for banking, email, and shopping. Different email addresses for different accounts. Limit cross-tracking.

Section 5

Protecting Your Social Media

Platform-by-platform privacy settings for the apps you actually use.

Facebook | YouTube | Nextdoor | General Safety Tips

Facebook — Lock Down Your Profile

01

Set Profile to Friends Only

Settings > Privacy > Who can see your future posts? Set to “Friends.” Then use Limit Past Posts to lock down everything you’ve ever shared.

02

Disable Face Recognition

Settings > Privacy > Face Recognition > toggle OFF. This stops Facebook from automatically identifying you in other people’s photos.

03

Review App Permissions

Settings > Apps and Websites. Remove any apps you don’t recognize. Old quizzes and games may still be harvesting your data years later.

04

Limit Who Can Find You

Settings > Privacy > How people find and contact you. Set phone and email lookup to “Friends” or “Only me.” Block search engines from linking to your profile.

YouTube & Nextdoor — Privacy for Seniors

01

Pause YouTube Watch History

myactivity.google.com > YouTube History > turn off. YouTube tracks every video to build a profile on you. Pausing stops the tracking.

02

Turn Off YouTube Ad Targeting

myadcenter.google.com > Personalized Ads > toggle OFF. You'll still see ads, but they won't be based on your browsing and watch history.

03

Nextdoor: Hide Your Address

Settings > Privacy > show only your neighborhood, NOT your exact street address. Nextdoor verifies your location but neighbors don't need your house number.

04

Nextdoor: Watch for Scams

Ignore DMs from strangers offering services. Never share financial info in neighborhood threads. Scammers use "local trust" to trick people.

Social Media Safety — Rules That Apply Everywhere

01

Never Post Travel Plans

Posting “Off to Hawaii for 2 weeks!” tells criminals your home is empty. Share vacation photos AFTER you return, not during the trip.

02

Ignore Friend Requests from Strangers

Fake profiles are used for romance scams and data harvesting. If you don’t know them in real life, don’t accept. Verify duplicate requests from “friends” by calling them.

03

Skip the Quizzes and Games

“What’s your celebrity name?” quizzes harvest your mother’s maiden name, pet name, and birth year — the same answers used for security questions on your bank account.

04

Turn On Login Alerts

On Facebook, YouTube, and Nextdoor: enable notifications for unrecognized logins. If someone accesses your account from a new device, you’ll know immediately.

Your Toolkit: Trusted Resources

privacyguides.org

The #1 recommended resource. Independent, non-profit, no ads. Covers every tool and topic from this presentation.

haveibeenpwned.com

Check if your email was in a data breach. Free, takes 10 seconds, created by a security researcher.

bitwarden.com

Free, open-source password manager. Works on all your devices. Recommended for beginners.

duckduckgo.com

Private search engine. Use instead of Google. Easy drop-in replacement, same quality results.

proton.me

Encrypted email, VPN, calendar, and cloud storage. Swiss-based. Strong privacy protections.

deleteme.com

Paid service that removes your info from data broker sites automatically. Well worth the annual fee.

The Bottom Line

You don't have to be paranoid. You just have to be aware.

Pick ONE thing from today and do it this week.

Todd Luttmers | Senior Financial Advisor | Keystone Private Wealth

Questions? Let's talk!

Reference: privacyguides.org