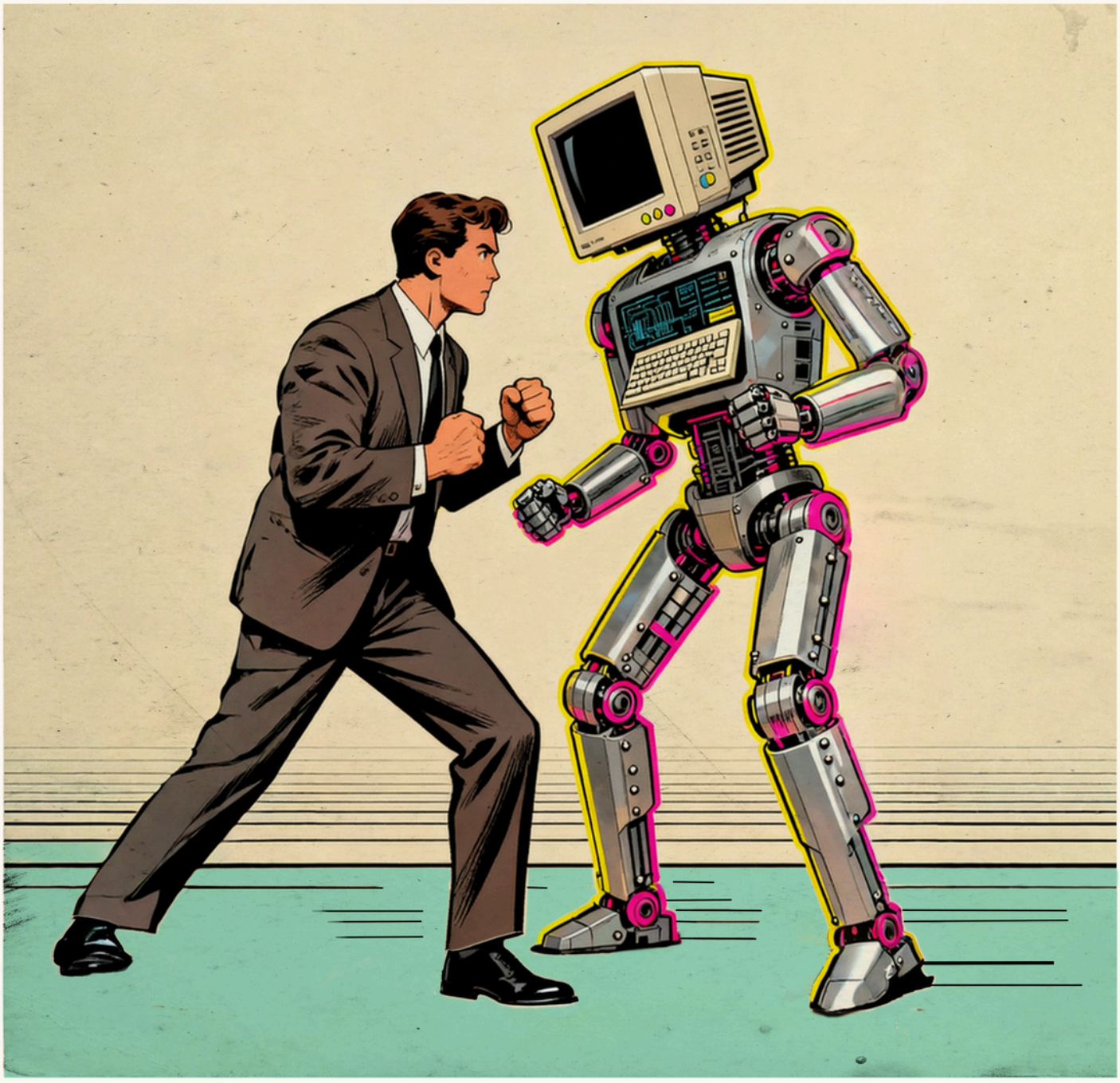
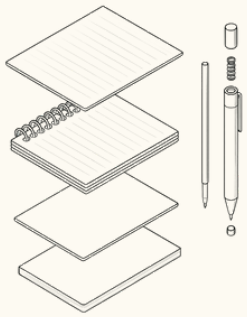
GROUP1001

Security Field Guide

A PRACTICAL APPROACH TO DIGITAL SELF-DEFENSE



/2025



Foreword

By taking time to open this guide, I'm already grateful. It means you care about protecting yourself, and by extension, helping protect Group 1001, its customers, its vendors and its employees.

Let's talk candidly about "the bad guys." They're not mythical villains hiding in the shadows or just names you hear in the news like *Scattered Spider* or *KungFu Kittens* (yes, those are actual threat group monikers). At the end of the day, attackers and fraudsters are real people. They behave like real people — with habits, goals, and limits. And just like any human, they're driven by return on investment. Their goal is speed and scale: how many people can they trick today, how much money can they steal this week? If building a detailed profile on you takes too much time, they'll move on to someone easier.

That's where you have real power.

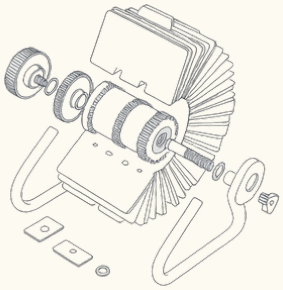
By making yourself harder to find and harder to exploit, you lower your risk, and the company's risk, dramatically. Think of it like locking your doors at night: no lock is perfect, but most burglars will bypass the house that looks difficult and go after the one that looks easy. Bad actors operate the same way. If it costs them too much time and effort to go after you, they'll turn their sights elsewhere.

The steps in this guide come from a place of thoughtfulness and care, and I hope you approach them with the same mindset. The guide is organized to match the themes from the training videos — covering email, finances, privacy, and more — so you can work through it step-by-step. Use it as a reference, return to it when you need it, and put it into practice at your own pace.

The world is indeed unpredictable, but none of us have to face it alone. By looking after ourselves and each other, we build the kind of security that keeps our people and our company protected.

Stay vigilant.

Amyn Gilani
AVP, Security Threat Intelligence Lead
Group 1001 Security Team

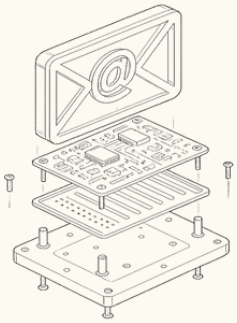


Owning Your Digital Footprint: How to Prepare

Locking down your digital footprint isn't a quick task, it's an ongoing project that takes time and effort, and frankly, it's never-ending. The reality is that most of us have already had our personal data breached multiple times, and attackers know it. Our information is scattered across the internet and it's being reused in ways that make scams more convincing than ever. This field guide will walk you through the steps, but it's important to understand a few key things up front:

- **It takes time and commitment.** Working through this guide isn't something you do once and forget. It requires regular attention and practice.
- **Family involvement matters.** Your security is tied to your kids, spouse, relatives, and even friends — their online activity can expose you, just as yours can expose them. **Invest time in working through this guide together and create a shared mindset of safe, cautious internet use.**
- **Skepticism is healthy.** Today, anyone can create convincing deepfake images, voices, and videos in minutes using free AI tools. **Never assume something is authentic just because it looks or sounds real.** By approaching emails, calls, and online interactions with caution, you make yourself much harder to manipulate.
- **Trust but verify.** Always double-check requests to move money, reset a password, or change account settings through a separate, trusted channel. Attackers often create urgency or fear and may even insist that *"no other method of communication is available"* to pressure you into acting quickly. **When in doubt, search online to see if others have reported similar scams, it can help guide your next step.**
- **Pause, take a breath, and ask for help.** If something feels off in a message or a call you've received, it likely is. Get a second set of eyes and get help from a trusted person. Don't be embarrassed, scams happen to everyone, and speaking up can save you trouble.

At the heart of this field guide is a simple truth: **your data is valuable because it represents you.** Owning your digital footprint means understanding its worth, taking responsibility for how it's protected, and knowing that small, consistent actions can make a big difference.



Protecting the Gateways of Your Digital Life: Email

Email is the backbone of your online identity — attackers know if they get into your inbox, they can reset passwords, intercept financial alerts, and impersonate you.

QUICK ACTIONS

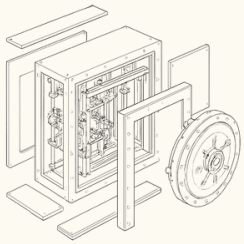
- **Turn on multi-factor authentication (MFA) where possible.** Using SMS for second-factor authentication is OK, but hackers can hijack your phone number and intercept those texts. True multi-factor authentication with an app like Google Authenticator or Microsoft Authenticator is much stronger. **Do That!**
- **Use a password manager.** Remembering dozens of complex passwords isn't realistic, and password managers solve this problem by securely storing and generating unique logins. Built-in options like **Apple iCloud Keychain** or **Google Password Manager** integrate directly with your devices, while trusted services like 1Password or BitWarden offer flexibility across platforms. These tools make strong passwords easy and eliminate the risk of reuse and can even alert you if your credentials are exposed in a breach. Ironically, password managers require a password, so be sure to use unique ones and change them every 60 days.
- **Protect your master keys.** Some credentials, like your password manager's master password or your crypto wallet's recovery phrase, unlock everything. Make them long, complex, and unique. Contrary to most advice, this is the one time you should write them down — but only on paper, and lock them away in a safe place. Never store them in email, notes apps, or the cloud.
- **If you're not using a password manager, never recycle passwords.** A single breach from one site can expose your email and trigger a chain of compromises across critical accounts, including banking. Aim for 12–16 characters, and use passphrases made of random words (like *RacecarCoffeeFeverBridge*) — they're easier to remember and far harder to crack than short, complex strings. Avoid small tweaks to old passwords (e.g., *Pacers2025* → *Pacers2026*), since attackers' tools guess those instantly.
- **Harden your recovery options.** Your recovery email and phone number are your lifeline if you get locked out, but they're also a target for attackers. Keep them current and secure and treat recovery accounts with the same care as your primary email. **If you use a loved one's account, make sure they understand that responsibility:** attackers may try to trick them into "helping" reset your account. A careless recovery contact can hand a hacker the keys, so choose wisely and keep everyone informed.

TUTORIALS – COMMON PROVIDERS

- **Gmail:**
  - Go to myaccount.google.com → **Security → 2-Step Verification → Get Started**
  - Add recovery email & phone under **Security → Ways to Verify**
  - Review suspicious logins under **Security → Your Devices**
- **Outlook/Hotmail:**
  - Go to account.microsoft.com → **Security → Advanced Security Options** → Turn on Two-Step Verification (Set up an authenticator app instead of SMS)
  - Add recovery email → **Security → Advanced options** → add recovery email
  - Review suspicious logins under **Sign-in Activity** to spot unusual logins
- **iCloud Mail:**
  - On iPhone: **Settings → [Your Name] → Password & Security → Turn On Two-Factor Authentication**
  - On Mac: **System Preferences → Apple ID → Password & Security**
  - Add recovery email: → ***Sign-In & Security*** **→ Account Security** → add recovery email
  - Review suspicious logins under ***Devices*** → review and remove any you don't recognize
- **Yahoo/AOL:**
  - Go to login.yahoo.com/account/activity → **Account Info → Security → 2-Step Verification** → add phone or app-based verification
  - Set up **App Passwords** for older mail apps that don't support MFA
  - Add recovery email: → **Add recovery email** → verify
  - Review suspicious logins under **Security** → review recent devices and locations → sign out of anything unfamiliar

EXTRA TIPS

- **Check forwarding rules regularly.** Hackers often set up hidden forwarding so your emails get silently sent to them.
- **Encrypt sensitive attachments.** Use built-in encryption (like Gmail Confidential Mode or Outlook encryption).
- **Review current log-ins.** Frequently review where you're signed in. If something looks suspicious, sign out everywhere, reset your password, and enable MFA.
- **Manage active sessions.** Use Gmail or Outlook's Recent Activity to see logins by location/device. If something looks suspicious, sign out everywhere, reset your password, and enable MFA.
- **Report phishing.** Use your provider's "Report phishing" button. This helps block future attacks.



Protecting Your Wealth

Your bank and payment accounts are the ultimate prize for criminals.

Fraudsters move fast, and once money is gone it's hard to recover. Protecting your finances means using the Core 3: complex passwords, multi-factor authentication, and account alerts. Apply these to banking and investment accounts, PayPal, Venmo, and crypto exchanges — and minimize daisy-chaining accounts together. Linking everything to your main checking account creates a domino effect if one service is breached. Instead, organize your cash flow to minimize exposure by using a separate account with limited funds, so a single compromise can't drain your savings.

TUTORIALS – COMMON PRACTICES

- **Explore your bank app's access and security features.** Every bank offers different tools — from login alerts and account change notifications to spending limits and fraud locks. Take a few minutes to review the security and privacy settings in your bank's app or website and enable features that add visibility or protection. These small adjustments often make the biggest difference in stopping fraud early, which is paramount.
- **Set up "high-risk" alerts.** Example: Notify me if a charge greater than $200 posts, or any international transfer occurs.
- **Link secondary checking accounts for payment apps and digital wallets.** Link Venmo, PayPal, Cash App, and crypto wallets to a separate checking account with **limited funds**. If one is compromised, the damage is contained, and your main savings stay protected. Most banks let you set up a no-fee secondary account in minutes, and it adds strong protection.
- **Wire transfers.** Always confirm instructions with a live phone call to a known number. Criminals excel at spoofing invoices and emails.
- **Check on your accounts frequently.** Spotting fraud early often means the difference between recovery and permanent loss. **Hunt for suspicious activity.**
- **Use official apps only.** Download from the App Store/Google Play, never from links in texts or emails. Bookmark your bank's site.

EXTRA TIPS

- **Money moves = red flag.** Legitimate banks and payment apps won't call and ask you to transfer funds. End the call and reach out through the official number on their website or app.
- **Avoid using or saving debit cards on e-commerce sites.** If that site is hacked, your checking account is exposed.
- **Review credit card statements line by line.** Fraudsters often start with small "test charges."
- **File your taxes early.** Criminals use stolen personal information to submit fake returns and steal refunds. Filing as soon as you have your documents reduces that risk. Be cautious of IRS impostor scams, fake government filing services, and even DMV-related scams, fraudsters often pose as official agencies to trick you into handing over money or personal data.
- **Be cautious with cryptocurrency.** Your **seed phrase** and **private keys** are the master keys to your wallet — never share them. Scammers often impersonate exchanges like **Coinbase**, claiming there's a problem with your account and asking you to "verify" or "recover" access. No legitimate company will ever request your keys. If contacted, stop and only use the official app or website to check your account.

Making Yourself Harder to Find on the Internet

Personally Identifiable Information (PII) Removal

When your personal information is exposed in a breach, it doesn't just disappear, it gets copied, resold, and recirculated for years. **Old breaches have a long tail, meaning data like your phone number, address, or Social Security number can resurface repeatedly, long after the original incident.** Criminals use this information to commit fraud, impersonate you, or build convincing scams. It's also why you likely see so much junk email, scam calls, and suspicious texts — your details are being traded and reused constantly. In some cases, exposed PII has even been used for harassment or physical threats.

The reality is that most of your personal information is already out there, and attackers will often know who you are before they ever contact you. It's impossible to erase yourself from the internet completely, but you can reduce what's exposed and avoid making it easy for criminals to find you.

This process requires diligence, and it's not a one-and-done task. It requires persistent attention as new data continues to surface.

QUICK ACTIONS

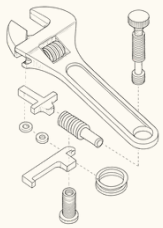
- **Google yourself to see how exposed you are.** Look for associated addresses, phone numbers, and sensitive details. Spend some time on this.
- **Remove yourself from data broker sites.** Start with Whitepages, Spokeo, BeenVerified, MyLife, and Intelius.
- **Check public records at the local, state, and federal level.** Many court filings, property records, voter registrations, and business licenses are published online and can expose your full name, address, or other sensitive details. **Start by searching your name in county clerk, tax assessor, or state court databases to see what's visible. Where possible, request redaction or removal**; some states allow you to mask personal details, especially for sensitive professions. If removal isn't possible, be aware of what's exposed and adjust what other personal data you share to limit how it can be used against you.

TUTORIALS FOR DATA BROKER CLEAN-UP: DIY VS. PAID

- **DIY:**
  - Use Google's "Remove Outdated Content" tool to request deletion of cached results.
  - Visit data broker opt-out pages (usually in the footer). Follow their process to remove your info.
  - Repeat every few months — they repopulate quickly.
  - Free resource for data removal: IntelTechniques Data Removal Workbook [Intel Techniques]
- **Paid:**
  - Services like DeleteMe, Optery, or Cloaked do this continuously for you, submitting removal requests across hundreds of brokers.

EXTRA TIPS

- **Reduce what you share going forward.** Oversharing creates new risks, even if you scrub old data.
- **Think like an attacker.** If someone wanted to impersonate you, what details could they find in 5 minutes? Remove those.
- **Schedule PII hygiene days.** Twice a year, search your info and clear out anything new.
- **For more education resources and dialogue on data privacy, visit:**
  - FAQ: r/privacy Guide to Online Privacy & Security [reddit.com/r/privacy]
  - Privacy Guides [privacyguides.org]



Tuning Up Your Social Media Privacy

Social platforms are the #1 source attackers use for profiling targets.

Every post, photo, or update adds to the picture of who you are, where you live, who you know, what you do, even when you're away from home. Criminals use this information to tailor scams, impersonate you, or launch fraud attempts that feel convincing because they're built from your own digital trail. The more personal details they collect, the easier it is for them to make that fake identity believable. **Limiting what you share, tightening privacy settings, and controlling your audience makes it much harder for attackers to gather intelligence and use it against you.**

It's not just your privacy at stake; your reputation is on the line too. A compromised or cloned social media account can be used to spread false information, harass others, or push scams in your name, damaging both personal relationships and professional credibility. In today's world, a single social media incident can have long-lasting consequences for you.

Take time to understand how social media platforms use and share your information.

QUICK ACTIONS

- **Visit your platform's Security and Privacy Center.** Take the time to explore every option and opt-in to features that strengthen your security and privacy. **These settings change often**, and new features are regularly added or rotated, so make it a habit to check back and adjust your preferences to stay protected.
- **Set accounts to Private.** Default to "Friends only."
- **Enable MFA on all platforms.** Facebook, Instagram, LinkedIn, TikTok, X, Snapchat.
- **Audit followers.** Remove people you don't know or trust.
- **Tighten old social media posts.** Criminals mine social media for details that help them build scams or impersonate you. **Go back through older posts and remove anything that gives away personal data**; birthdays, addresses, school names, travel plans, or family details. Photos can be just as revealing; houses, license plates, or even the background of a picture can be used to track where you live or work.

TUTORIALS – POPULAR PLATFORMS

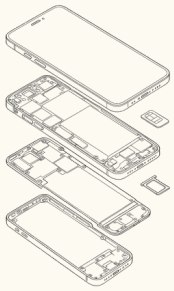
- **Facebook:** Run **Privacy Checkup** (Settings & Privacy → Privacy Checkup). Limit who can look you up by phone/email. Turn off "search engines linking to profile."
- **Instagram:** Profile → Settings → Privacy → Switch on **Private Account.** Limit story viewers.
- **LinkedIn:** Review your LinkedIn visibility settings and check what's being shared, adjust to your comfort level, and tailor access so only the right audience sees your information: **Me → Settings → Visibility**
- **TikTok:** Profile → Settings & Privacy → Privacy. Set Comments, Mentions, DMs, Duets, and Stitches to **Friends or No one.**
- **Snapchat:** Settings → Privacy Controls. Enable **Ghost Mode** on Snap Map. Set "Contact Me" to **Friends only.**
- **X (Twitter):** Settings → Privacy & Safety → Audience & Tagging. Switch on **Protect Your Tweets.**

EXTRA TIPS

- **Be wary of your social media connections.** Most scams start with compromised social media accounts, where attackers use your friend network to gain trust. If a "friend" asks for money online, treat it as suspicious. If your friend needs money, have them call you.
- **Be selective when choosing your profile picture.** When possible, limit what's public and consider using a profile photo that doesn't clearly identify you or your family.
- **Don't overshare travel plans.** Criminals use this to time attacks when you're distracted or away from home.
- **Set up recovery and legacy options.** Make sure your accounts have updated recovery emails and phone numbers in case you're ever locked out. For platforms that offer it, assign a legacy contact so a trusted person can manage or close your account if you pass away.
- **Control who sees your posts.** Use "close friends" lists or audience controls to limit visibility, a**nd if you want a public presence, consider maintaining two profiles**; one for professional/public sharing and another kept private for friends and family.
- **Report impersonation quickly.** Impersonation is when a fraudster poses as you, or someone close to you, to trick others into sending money, soliciting information, or granting access. **Every platform has an impersonation reporting tool.**
- **Be careful with "social logins."** Logging into other apps with Facebook or Google shares more data than you realize.
- **Review where you're logged in from.** Check your active sessions under Settings → Security. Log out devices you don't recognize and change your password immediately.

WATCH OUT FOR THESE SCAMS

- **Marketplace Scams.** Fraudsters exploit platforms like Facebook Marketplace or Instagram shops by creating fake listings, requesting payment outside of the platform, or shipping counterfeit/never-delivered goods. Red flags include offers that are "too good to be true," insistence on fast payment, or reluctance to meet in person for local deals.
- **Impersonation Scams.** Criminals create fake accounts using your name, photos, or stolen information to trick your friends, family, or coworkers into sending money or clicking malicious links. Red flags include duplicate friend requests, urgent requests for financial help, or messages that feel "off" compared to how the real person normally communicates.
- **Romance Scams.** Fraudsters build fake relationships over weeks or months, often using stolen photos and scripted conversations. Eventually, they ask for money to cover "emergencies," travel expenses, or investments. Red flags include refusing to meet in person, avoiding video calls, and always having an excuse for why they need money.
- **Giveaway & Investment Scams.** Attackers promise free prizes, crypto doubling, or "guaranteed" investment returns, often impersonating real brands or influencers. They ask for payment upfront, personal details, or wallet access. Red flags include requests for fees to claim a prize, unrealistic returns, or links that take you off the official platform.
- **Job/Work-From-Home Scams.** Fraudsters advertise fake remote jobs or "side hustles" through social media posts or messages. They may ask for personal details, upfront fees, or request you deposit checks and transfer money. Red flags include jobs that sound too easy, high pay for little work, or requests for bank account info early in the process.
- **Sextortion.** Attackers may trick or pressure someone into sharing intimate photos or videos, then threaten to release them unless money is paid. Warning signs include strangers suddenly sending explicit content, quickly escalating conversations, or asking you to move to a private platform. If this happens, stop all contact, don't pay, and report the account immediately. This scam is also frequently seen on gaming platforms, where attackers use chat features to target younger players.



Protecting the Gateways of Your Digital Life: Phone

Your phone is the master key. Protect it.

Your phone is more than a device; it's the key to your identity. If criminals take over your number or your device, they can reset passwords, intercept messages, and break into your bank, email, and social accounts within minutes. Hardening both your phone and your number is critical. ***All carriers offer unique features to help prevent SIM swapping, so take the time to research and enable them.*** By locking down carrier settings, strengthening device security, and reducing reliance on SMS for authentication, you make it far harder for attackers to use your phone as the wedge into your digital life.

QUICK ACTIONS

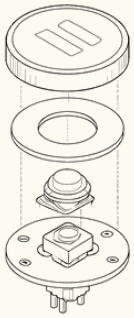
- **Start with your carrier's security settings.** Every major carrier offers tools to protect against SIM swaps, but most people never turn them on. Log in to your carrier's app or website and look under Security or Account Settings. Add a PIN, passcode, or "number lock" to your account so no one can move your phone number without it. If your carrier offers extra features like "account takeover protection" or "port freeze," enable them. These steps are your first line of defense.
- **Lock down your phone itself.** Use a strong device passcode (not 1234, not your birthday), and enable biometric login (Face ID or fingerprint). This prevents a stolen phone from being used to reset accounts.
- **Disable unused features tied to your number.** Turn off voicemail PIN resets, call forwarding, or text-to-email if you don't use them. Attackers often exploit these weak links.
- **Use secure backup options.** Make sure your iCloud or Google account has MFA enabled and its own strong password. If criminals hijack your cloud identity, they can take control of your phone and number together.
- **Audit where your number is used.** Your phone number should not be the default login or recovery option for every account. Replace SMS-based recovery with authenticator apps or email where possible.
- **Act fast on red flags.** Unexplained loss of service, new devices tied to your cloud account, or unfamiliar SIM activity are signs of takeover. Connect to Wi-Fi, lock your account, and call your carrier immediately.

TUTORIALS – MAJOR CARRIERS

- **AT&T:** Call 611 or log in → Set up an **Extra Security PIN** (required for SIM swaps or account changes).
- **Verizon:** Log in to My Verizon → Account Settings → Security → Enable **Number Lock** to block unauthorized SIM changes.
- **T-Mobile:** Log in to My T-Mobile → Profile → Account Security → Add a **PIN/Passcode.** Call support to enable **Account Takeover Protection.**
- **Other Carriers:** Look for a **PIN, port freeze, or number lock** option in account security settings, or call customer service.

EXTRA TIPS

- **Update promptly.** Phones and apps receive regular patches for newly discovered vulnerabilities. **Turn on automatic updates so you're always protected without having to think about it.**
- **Use Wi-Fi carefully.** Public Wi-Fi can be monitored or spoofed. Stick to your mobile network for sensitive tasks.
- **Back up safely.** Regularly back up your phone to iCloud, Google Drive, or an encrypted local copy. If your device is lost or compromised, you can recover quickly.
- **Check where you're logged in from** in your Apple ID or Google account and remove devices you don't recognize.
- **Enable carrier alerts** for SIM changes or port-out requests — early warning is critical.
- **Silence unknown callers and texts.** Most scams start with calls or messages from numbers you don't recognize. On iPhone and Android, you can enable settings to block or silence unknown numbers, so they are sent directly to your voicemail or filtered into a separate folder.



Freezing Your Credit

A credit freeze is the single most powerful step to stop identity theft.

Freezing your credit is one of the most effective ways to block identity thieves from opening new accounts in your name. The process is free, but it does require you to set up a PIN or password with each bureau. **If you plan to apply for new credit, planning is key, you'll need to temporarily "thaw" or unfreeze your credit, which can be scheduled in advance.** It's a small inconvenience compared to the protection it provides. You may be prompted to upgrade to premium services, but a credit freeze itself is free and you don't need to pay for additional features to secure your credit.

QUICK ACTIONS

- **Freeze with all three major bureaus.** Equifax, Experian, TransUnion (plus Innovis).
- **Check your credit report regularly.** Each credit bureau gives you one free report per year, available directly through their official sites. Avoid third-party services that try to charge you — go straight to the source for accurate, no-cost reports.

TUTORIALS – HOW TO FREEZE YOUR CREDIT

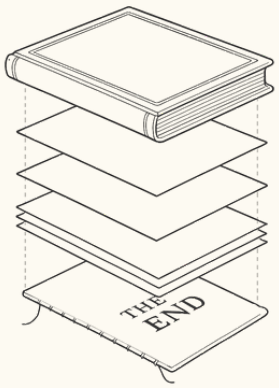
- **Equifax:** equifax.com/personal/credit-report-services/credit-freeze/ → Place Security Freeze → Complete Form → Verify Account via Email → Sign-in → Freeze Credit
- **Experian:** experian.com/freeze/center → Complete Form → Verify Account via Email → Sign-in → Freeze Credit
- **TransUnion:** transunion.com/credit-freeze → Complete Form → Verify Account via Email → Sign-in → Freeze Credit
- **Innovis:** innovis.com/securityFreeze → Complete Form → Verify Account via Email → Sign-in → Freeze Credit

Each bureau requires setting up an online account or phone **PIN.** Keep this information safe, you'll need it to lift or manage the freeze.

EXTRA TIPS

- **Freezes are free.** They don't impact your credit score.
- **Scheduled and Temporary lifts.** Use your PIN to unfreeze when applying for a mortgage, car loan, etc. You can schedule these ahead of time.
- **Family protection.** Freeze credit for children and elderly relatives — fraudsters target them because no one is watching.

Conclusion



We've covered a lot in this guide, but the most important takeaway is simple: you have more control over your digital safety than you might think. Every action you take, whether it's securing an account, limiting what you share, or pausing before you click, makes you less of a target and more resilient in the face of threats.

Your efforts matter, and together we're creating a safer environment for everyone.

Sincerely,
Group 1001 Security Team
Security@Group1001.com

DISCLAIMER

This Field Guide is provided for educational and informational purposes only. It does not constitute legal, financial, or professional advice, and should not be relied upon as such. While the information is intended to help you make safer choices online, Group 1001 makes no representations or warranties as to the completeness, accuracy, or suitability of the content and cannot guarantee outcomes or be held responsible for how it is used. For advice regarding specific circumstances, please consult with a qualified professional.

References to security services, technologies, or companies are included solely for informational purposes. Group 1001 does not endorse, sponsor, or warrant any third-party products, services, or practices mentioned herein, nor is any content intended to disparage or criticize other organizations.