



Personal Protection from CyberCrime

Now with AI Scam Protection

Second Edition

Personal Protection from CyberCrime

Foreword by Chase Cunningham

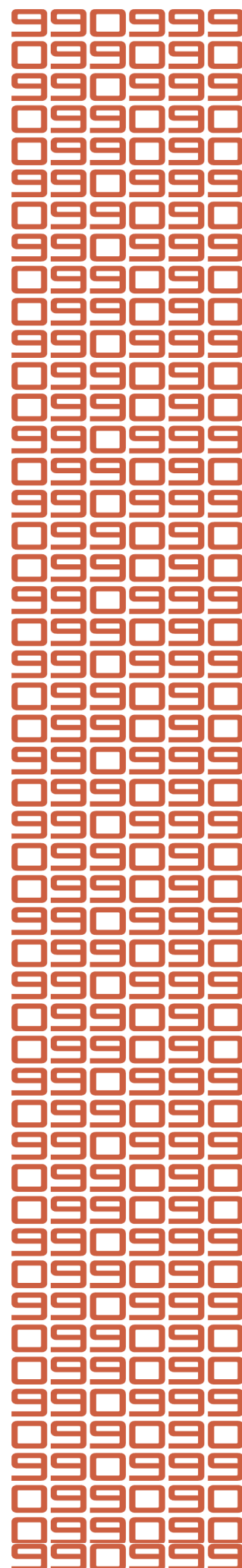
Let's face it—cybercrime isn't just something that happens to large corporations or the tech-savvy. It's not a distant threat, but a pervasive one, lurking at the edges of your Wi-Fi connection, eyeing your email inbox, and waiting when you click "Sure, I accept cookies" without thinking twice. But here's the thing: protecting yourself from cybercrime doesn't have to be an arduous task.

In today's hyper-connected world, where even our refrigerators want to be on the internet, cyber threats are a reality for everyone. We're talking about data breaches, identity theft, phishing attacks, ransomware—the list is longer than your Netflix queue. But while these threats are everywhere, so are the tools to protect yourself, and, spoiler alert: you don't need a PhD in computer science to do it. These tools are within your reach, empowering you to take control of your digital security.

Cybersecurity, at its core, is about making life just a little harder for the bad guys—and that's not as hard as it sounds. It's like locking your front door and not leaving your wallet on the dashboard when you park your car. Well-applied, basic security principles—like using strong passwords, avoiding sketchy links, and updating your software occasionally—are all necessary to create a solid defense. These are simple measures that anyone can implement, and they can make a significant difference in your digital security.

The goal of this book isn't to turn you into a hacker's worst nightmare (though that would be cool). It gives you the tools to stay one step ahead of today's cyber threats without feeling like you've entered the Matrix. You don't have to wear sunglasses at your keyboard to feel secure, but a little awareness and a few well-placed protections can make all the difference between a peaceful night's sleep and a frantic call to your bank.

So, buckle up, keep your guard up, and remember: in the digital world, staying safe isn't about being perfect; it's about being prepared. Let's make sure the cybercriminals swipe left on you.



Introduction

Years ago, I was at a hacker conference in Las Vegas called @DEFCON. During a session in the @SocialEngineeringVillage an awesome social engineer said, “Stop delivering the same lame corporate training to your company’s employees”. She said, “Teach them how to protect themselves and their families.” That struck a chord with me, like an A-Sharp (for the musical folks). In large enterprises, we deliver training, which is usually required annually for compliance reasons. But, it’s lame and boring, and as such, most people have it running in the background while they ignore it and do some real work.

In the end, we all care about our personal stuff way more than our employers. I like my bank account to have money. Or, when there’s none, it’s because I bought lots of music gear.

That’s what led me to write this document. Something that you can use at home. Some simple education. It is also something that doesn’t require an IT degree to understand. Plain English, or in my case, a bastardized Scottish-American vibe... anyway, I’ll try to keep it easy.

Den Jones

Founder & Chief
Executive Officer,
909Cyber



What’s New in the Second Edition

A lot has changed since our First Edition in late 2024... mostly because the bad guys got a new toy called AI. Scams now come with perfect grammar, cloned voices and fake video. So we rewrote our AI section from scratch, added passkeys, SIM swap protection and a family “safe word”, refreshed every link, and finished with a one-page checklist you can actually tick off. Look for the **NEW** tags.

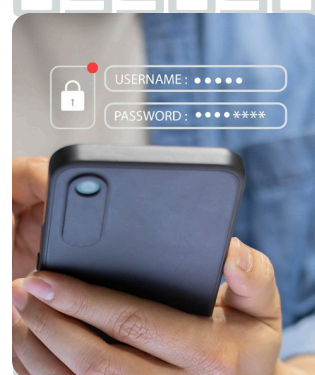
Identity 101: A Quick Lesson

Before we start, when you use most apps, services, and websites, they want to know it’s you. So, they ask you to create an account. This requires a bunch of information, but the core thing is a username and password (or, more and more, a passkey... more on that later). This is so they know it’s you.

A username obviously has to be unique since it’s only tied to you. The most common way to do this is to use an email address, but some companies still use a username that you or they create, and your email address is then separate (this is with the idea you may wish to change email over time). The password is then something you create; which as we explain below should be unique to that account and not re-used.

Apps, services and websites have collected a wide range of personal identifiable information (PII) on each of us, including, but not limited to, our government IDs, Social Security numbers, driver’s license numbers, home addresses, health information, financial information, relatives’ names, pet names and much, much more.

Often, when an app, service, or website is hacked or compromised, the personal information that has been collected on its customers is stolen, traded, or sold by the hackers. And today, that stolen information gets fed into AI tools that help criminals write scams aimed squarely at you.



Browser Plugins: A Quick Lesson

Web browsers... you may just know them as Google Chrome, Microsoft Edge, Safari, Firefox, Brave, DuckDuckGo, Opera and a few more. For most of us web browsers are how we access the internet and almost all of the applications that run on the internet.

What's good to know is that every browser includes the ability to install mini-applications called "plugins" or "extensions." These are small applications that add features and functionality enabling the web browser to have added capabilities.

Good examples are things like Grammarly, a password manager, Google Translate and ad blockers. These are all great little applications that help you, but make sure you download them from reputable sources.

A word on AI extensions NEW

"AI assistant" and "ChatGPT for Chrome" style extensions are everywhere. Many can read every page you visit, including your email and banking. Fake ones are a popular way to steal data. Only install them from the official company, and only if you really need them.

So, the main point here is: browsers and any browser plugins should only be installed from trusted, reputable sources. Every so often, open your browser's extensions page and remove anything you don't use.



Signs of a Scam

Scammers use so many methods these days; could be legitimate sites like LinkedIn or embedded in a paid advert in your favorite news source. Text messages, messenger applications (e.g. WhatsApp, Telegram & FB Messenger), phone calls, video calls and even QR codes.

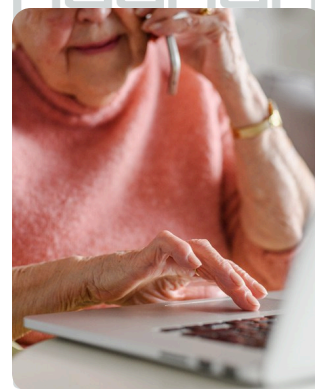


There was a case where what appeared to be a reputable post on obtaining a lower mortgage rate resulted in the excited user clicking the link to a malicious site. Which of course prompted the unsuspecting user to enter some detailed information which included their Social Security number and bank details. Of course it looked like a reputable bank.

It's no longer the prince of Nigeria asking for some money ;-)

The reality is there are common themes to any scam; at a high level these tend to be:

- The call, the email or the text was received when you didn't expect it.
- There was a sense of urgency (do it now otherwise... we'll cut off your gas, your phone or whatever).
- They want to move the conversation to another app, like WhatsApp, Telegram or Signal.
- NEW Someone contacts you and says they are sending you a code (text message/SMS) or asks you to share a code from an authenticator app. Nobody legitimate will ever ask for that code.
- They ask for payment in gift cards, crypto, wire transfers or Zelle (this is common in a small business setting too).



- Websites selling goods and services; if it's too good to be true... well, you know that saying. One thing to watch out for is if they say they are unable to collect the item but they'll pay more upfront for a courier. They give you extra for your trouble and include the courier fee; but then want you to pay the courier via Zelle or Venmo. Then you later find out their money did not clear and you've lost the money you sent the courier.
- Includes a link to click and sometimes they look so real:
 - **Spot the Difference?**
maybank2u.com ✓ is not the same as **maybank2u.com** ✗
citibank.com ✓ is not the same as **citibank.com** ✗
 (The first one is correct, the second one is from hackers.) The "a" in the latter URL is a Cyrillic character. An average user can easily fall for this. Beware of any message requiring you to click a link. **Please Stay Alert!**

Perfect Grammar Is No Longer a Good Sign NEW

We used to say "look for bad spelling." Forget that. AI now writes flawless emails and texts in any language, in the voice of your bank, your boss or your kid. Judge a message by what it asks you to do, not by how well it's written.

A golden rule: Microsoft, Apple and Google will never call you to say your device has a virus or has been compromised. Neither will your bank ask you to "move your money to a safe account."

Some pesky examples in recent months:

- Email from a bank I don't use.
- Text messages about unpaid road tolls or a delivery I'm not expecting (or that requires payment for delivery).
- QR code stickers placed over the real ones on parking meters and restaurant tables, leading to fake payment pages.
- Random strangers liking your social media posts, usually someone of the opposite sex, and if you look at their profile they have almost no followers or posts. Their goal is for you to get excited cause you think they're hot and reach out to them. **Don't.**

How to Protect Yourself?

Links to Websites

Instead of clicking the link, visit the official website by typing the address yourself or using a saved bookmark.

Phone Calls

Ask for their details; if they give you a number, write it down, but don't call it (or trust it). Look up the official phone number for that business (via their website or the back of your card); then call that number. Caller ID can be faked.

Social Media

Simple steps include going to privacy settings and making your profile only visible to your connections (private, not public). The less of your face and voice that's public, the harder it is for AI to copy you.



If You Only Do Four Things

If you only took away four things from this document I'd say do a **Credit Freeze**, start using a **Password Manager** and **Multi-Factor Authentication (MFA)**, and agree on a **Family Safe Word** **NEW** today.

Credit Freeze and Credit Thaw (United States)

What is it?

Credit has been popular since the 1970s, but it's not just consumers who love it; hackers do, too. In 2025, Americans reported more than \$20 billion in cybercrime losses to the FBI, and people over 60 alone lost more than \$7.7 billion. Your credit can be misused in many ways. Chances are your personal information will be (or has been) compromised.

What risk does it solve?

Freezing your credit is free and prevents someone from using your stolen information to open credit accounts or loans in your name, protecting you from potential debt, loss of property, or even bankruptcy.

How to use:

- Visit [Experian](#), [Equifax](#) and [TransUnion](#).
- Create accounts using a strong password and enable Multi-Factor Authentication (strong passwords, managing passwords, and MFA are also discussed in this document).
- You'll need to provide personal information (like Social Security number, birth date, address) to verify your identity.
- Follow the steps by each bureau to freeze your credit.
- When applying for new credit, log in to "thaw" your account. Thawing can take up to 24 hours, so plan ahead. Afterward, refreeze your credit or set a time period for it to automatically freeze again.

Go a step further **NEW**

- **Freeze your kids' credit too.** Children have clean credit files, which makes them a favorite target. All three bureaus let parents freeze a child's credit for free.
- **Get an IRS Identity Protection PIN.** A free six-digit PIN that stops someone filing a tax return in your name. Sign up at irs.gov/ippin.
- **Freeze the lesser-known bureaus.** [ChexSystems](#) (used for opening bank accounts) and [Innovis](#) also offer free freezes.

Important:

A credit freeze is free, and you don't need to pay for extra services, which may sound more secure but aren't necessary.



Fraud Alert:

In addition to the credit freeze, you can also add a free “fraud alert” to your credit report. It lasts one year and can be renewed; placing it with one bureau automatically adds it at the other two.

Adding a fraud alert above and beyond the credit freeze provides additional proactive protection. While a credit freeze locks your credit file, the fraud alert indicates to creditors that additional verification is required before issuing any new credit. The fraud alert is a good tool to help prevent identity thieves from opening accounts in your name, even if they have your personal information.

Password Manager

What is it?

How many passwords do you have? How often do you reuse them? A good password manager helps you use unique passwords for every account, so your bank password isn't the same as your Netflix or Walmart login.

What risk does it solve?

When companies get breached, hackers try stolen usernames and passwords on other websites. If you reuse the same credentials, it's an open door for them. Password managers protect you by storing unique, strong passwords and can also save time by automatically filling in forms. A bonus: a password manager won't autofill your password on a fake lookalike website, which is a great early warning that something is off.

Our picks for password managers:

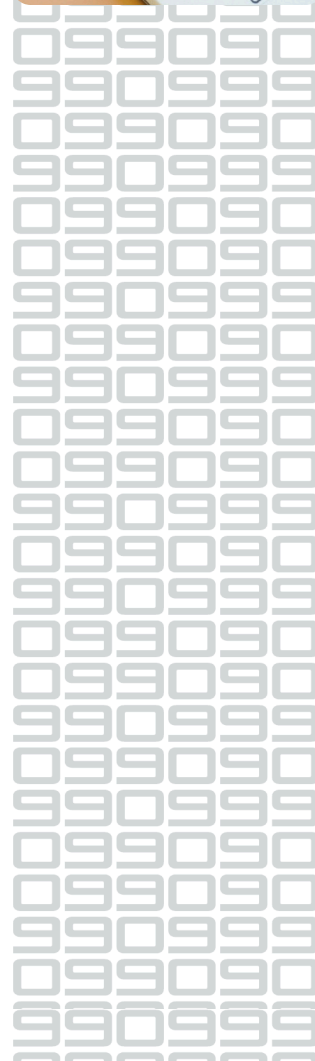
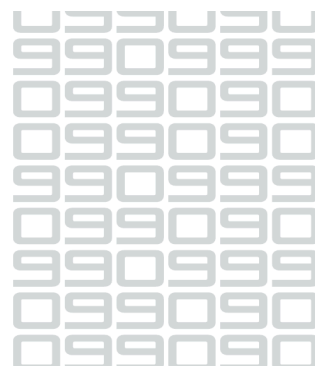
[1Password](#), [Dashlane](#), [Keeper](#), [Bitwarden](#)

How to use:

Download and purchase from the provider's website or your device's app store. On computers, install the browser plugins to sync passwords across all browsers and devices, even when using different browsers.

A few features that we love are:

- **Compromised Account Alerts:** A dashboard shows accounts that might be compromised.
- **Password Generator:** Helps create strong, unique passwords without needing to remember them.
- **Passkey Storage:** Saves and syncs your passkeys across devices (see below).
- **Multi-Factor Authentication (MFA):** Adds an extra layer of security by requiring a second form of authentication beyond just the password.
- **Syncing Across Devices:** Install the manager on all devices and browsers for seamless access.
- **Password Sharing:** Share passwords securely with others using the same manager.
- **Secure Info Storage:** Stores personal info for auto-filling forms like shipping or account details.



Passkeys: Goodbye Passwords NEW

A passkey replaces your password with your face, fingerprint or device PIN. There's nothing to remember, nothing to type, and nothing a scammer can trick you into handing over, because a passkey only works on the real website it was made for. Google, Apple, Microsoft, Amazon, PayPal and many banks now support them.

How to use: when a site offers "Create a passkey" (usually under Security settings), say yes. Your phone or password manager stores it and syncs it to your other devices.

Alternatives:

Operating systems like Windows, macOS, iOS, and Android, as well as browsers like Chrome and Firefox, offer built-in password management. If you switch between browsers and platforms or want more advanced features, a dedicated password manager is a better option.

We nearly included Apple's Passwords app in the recommended list above. It's built into iPhone, iPad and Mac, works on Windows through iCloud, handles passkeys and verification codes, and allows password sharing with family. At this time it doesn't store secure documents, credit cards, passports and other personal information the way the dedicated managers do.

Different Email Addresses for Different Purposes

What is it?

Just like having different passwords for each site, using different email addresses for different purposes significantly improves security. While having multiple email accounts may seem impractical, even separating them for key purposes can make a huge difference.

What risk does it solve?

Using different email addresses based on purpose helps increase security, reduce phishing risks, and limit the damage if one account is compromised.

How to use:

Method 1: Two Lanes

- General Email (first.last@email.com): for most apps, services, and websites. Especially for mailing lists, discounts, coupons etc.
- Financial Email (nothing.that.ids.you@email.com): for banks and financial sites only.
- How it helps: when an app using your general email is compromised, attackers don't have access to your banking email or passwords. Any emails pretending to be from a bank that arrive in your general inbox can be safely ignored.

Method 2: Three Lanes ADVANCED

- Primary Email (first.last@email.com): for personal correspondence and important services like your doctor or phone carrier.
- Financial Email (nothing.that.ids.you@email.com): for banking and financial sites.
- Secondary Email (first.randomnumbers@email.com): for apps, services, and websites not linked to your primary or financial accounts.



- How it helps: it adds an extra layer of isolation from Method 1. Any unexpected emails in your primary inbox can be safely ignored.

Method 3: Masking **VERY ADVANCED**

- Primary Email (first.last@email.com): for personal correspondence and important services.
- Financial Email (nothing.that.ids.you@email.com): for banking and financial sites.
- Masked Emails: use services like Apple's "Hide My Email," 1Password's masked email, [Firefox Relay](#), [DuckDuckGo Email Protection](#) or [SimpleLogin](#) to create a unique email for every app and website. These forward to your primary account.
- A note on Gmail's "+" trick (username+website@gmail.com): it's handy for filtering and for spotting who sold your address, but it still shows your real email to anyone who looks. It's a filter, not a mask.
- How it helps: when an app or website is breached, the attacker doesn't know any of your other emails or other accounts. You can also safely ignore any financial-related emails that land in your general inbox.

Conclusion:

By using different email addresses for different purposes, you significantly reduce the risk of phishing and identity theft. It not only helps protect sensitive accounts like your bank or investments but also makes it easier to spot suspicious activity. Implementing even a simple two-lane system can strengthen your overall security without being overwhelming. Small changes like this can go a long way in keeping your data secure.

Multi-Factor Authentication (MFA)

What is it?

Multi-Factor Authentication (MFA) adds an extra layer of security to your accounts. It requires not just a password, but an additional form of verification (like a text message code, an authenticator app, a passkey, facial recognition or fingerprint) before allowing access.

What risk does it solve?

Passwords are often stolen during data breaches and can be guessed, making it easier for attackers to access your accounts. MFA ensures that even if someone has your password, they still can't log in without the second form of verification. This dramatically reduces the risk of unauthorized access and protects your personal data from being stolen.

How to use:

- Set up MFA on your accounts, especially your email, banking, mobile phone carrier, AI tools and social media accounts. Most websites and apps offer this feature in their security settings.
- Choose the strongest second factor the site offers. From best to "better than nothing":



Option	Why
1. Passkey or security key	Can't be phished; only works on the real site. Security keys like YubiKey are a small USB/NFC device.
2. Authenticator app	A code from an app like Google Authenticator, Microsoft Authenticator, Authy or Ente Auth. Much harder to intercept than a text.
3. Text message (SMS)	Better than no MFA at all, but criminals can intercept it or steal your number with a SIM swap (see Protect Your Phone).

- **Log in securely:** once MFA is set up, you'll enter your password first, then verify your identity using the additional factor.
- **Never approve a prompt you didn't start.** **NEW** Criminals who already have your password will spam you with "Is this you signing in?" notifications, hoping you'll tap Yes just to make them stop. If you didn't just try to log in, tap No and change that password.

Limit Bank/Debit Card Use

What is it?

Your ATM, debit or bank card is directly linked to your bank account and usually requires a PIN (4 to 6 digits) for transactions.

What risk does it solve?

Using a debit card with a PIN is considered an approved transaction, so if someone copies your card through skimming or hacks a payment system, it can be difficult to prove fraud and get your money back. Instead, consider using credit cards, virtual credit cards, or digital wallets like Apple Pay or Google Pay.

How to use:

Limit your bank card use to your bank branch, preferably at the teller or indoor bank machines when possible. We won't cover how to apply for credit cards or add them to virtual wallets in this article. However, using virtual wallets like Apple Pay or Google Pay is safer than using a bank or credit card alone. You can take security a step further by using services like privacy.com to create virtual credit cards for online purchases. These cards can be single-use or multi-use, with spending limits, and block fraud or overcharging.

Turn on instant alerts. **NEW** Every banking and credit card app can text or notify you for every transaction. It costs nothing and means you'll spot fraud in minutes, not at the end of the month.



Avoid Public WiFi

What is it?

Public WiFi, like at coffee shops, airports, hotels or restaurants, is not secure or monitored for hackers. Anyone on the same network, or worse, controlling it, can attempt to attack your device, set up a fake network with a similar name, or trick you into entering your login details on a fake sign-in page.

What risk does it solve?

Avoiding public WiFi reduces your risk of being targeted by hackers who may try to access your device or trick you into sharing sensitive information.

How to [not] use:

The safest alternative is to tether your laptop to your mobile device, or simply use your mobile device's cellular data without connecting it to public WiFi. Stick to trusted networks like your home, work, or private WiFi. If you must use public WiFi and can't rely on a cellular signal, a Virtual Private Network (VPN) can provide some protection, but a VPN doesn't eliminate all risks. And whatever network you're on, avoid banking or shopping on it if you can wait.

Alternatives:

- **Virtual Private Network (VPN):** encrypts your internet traffic and routes it through a private server, helping to protect your online activity. However, VPNs can't fully protect you if a hacker controls the network you're on.
- **Firewalls:** these monitor and block unauthorized network traffic to your device. Both Windows and macOS have free, built-in firewalls that can be enabled easily, but they won't fully protect you from a hacker-controlled network.
 - Windows 11: go to Settings > Privacy & security > Windows Security > Firewall & network protection, and make sure the firewall is on for your active network.
 - macOS: go to System Settings > Network > Firewall, and turn it on.
- **Check the padlock and the address:** make sure sites you log in to start with https:// and the address is exactly right. The free [CheckMyHTTPS](#) browser extension can also warn you if your secure connection is being intercepted, decrypted, listened to, or modified.
- **Forget networks you're done with:** tell your phone and laptop to "forget" coffee shop and hotel networks so they don't auto-join a fake one with the same name later.

Helpful Links:

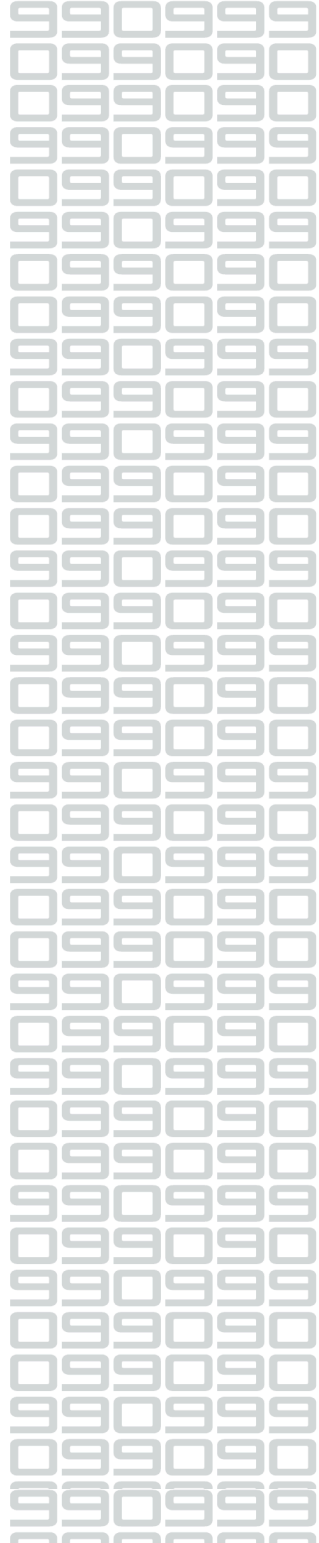
[FREE] Built-in Firewall How To's

- [Microsoft Windows](#)
- [Apple macOS](#)

[PAID] VPN Services

When using a VPN, it's important to pair it with a firewall for added security. If the public WiFi network doesn't allow VPN, disconnect from the public WiFi network.

- [NordVPN](#)
- [Surfshark](#)
- [ProtonVPN](#)



Conclusion:

Using public WiFi increases your vulnerability to attacks, so it's best to avoid it when possible. Stick to using your mobile data or a trusted network. If public WiFi is your only option, a VPN can offer some protection, but pairing it with a firewall and secure website checks can help further reduce risks. Keep in mind that no solution is foolproof when using public networks, so it's essential to stay cautious.

Protect Your Phone

What is it?

Your mobile phone stores a lot of personal and sensitive information, such as bank account details, access to your password manager, your MFA codes, photos, and other personal data.

What risk does it solve?

Since your phone holds so much critical information, it can be a single point of attack, or failure. Protecting it is essential to prevent theft and cybersecurity breaches.

How to use:

- Set a 6-digit (or longer) PIN, thumbprint, or Face ID to unlock your device.
- Consider disabling your thumbprint or Face ID when traveling, and rely only on your PIN. In some places, at some borders, you can be compelled to unlock a phone with your face or finger more easily than with a PIN you know.
- Never store passwords in Notes or Photos.
- Turn on automatic updates, and install them promptly. Most updates fix security holes that criminals are already using.
- Regularly back up your device.
- Review app permissions now and then; does that flashlight app really need your contacts and microphone?
- Set up stolen device protection:
 - [Apple iOS: Stolen Device Protection](#)
 - [Android: Theft Detection Lock](#)
- **Lock your phone number with your carrier.** **NEW** In a "SIM swap," a criminal convinces your carrier to move your number to their phone, then receives all your text message codes. Add an account PIN and turn on your carrier's protection (T-Mobile SIM Protection, Verizon Number Lock, AT&T Wireless Account Lock).
- If you're a likely target (public figure, executive, journalist), Apple's Lockdown Mode and Android's Advanced Protection add serious extra hardening.
- Avoid public WiFi (as mentioned elsewhere in this document). For extra security, consider disabling WiFi on your device when not at home or work.



Malware Protection

What is it?

Over the years, it's been called Anti-Virus and Anti-Malware, and in the media, acronyms like EDR (Endpoint Detection and Response).

What risk does it solve?

When you click links or download email attachments, sometimes there's malicious code that can compromise your device, often using your device to launch attacks or steal your data. Every day we're exposed to emails that entice us to click links and web advertisements (even within legitimate sites) with an aim to install software on your device.

Our Guidance:

Most major computers, tablets, and phones come with built-in free software that is decent enough, so using additional third-party software is optional. Be aware that some vendors will scare you into thinking that you need their paid-for software and services, which is fine for the more paranoid person.

The #1 thing you can do: turn on automatic updates. For your computer, phone, browser and apps. Updates close the holes that malware uses to get in.

Still on Windows 10? NEW

Microsoft ended free security updates for Windows 10 on October 14, 2025. A computer that no longer gets security fixes gets more dangerous every month. Upgrade to Windows 11 if your PC supports it, enroll in Microsoft's Extended Security Updates as a stopgap, or plan to replace it.



AI: The Scammer's New Toolkit NEW

Remember when you could spot a scam by the bad spelling? Those days are gone. AI now writes perfect emails, clones voices from a few seconds of audio and makes fake videos that look like the real thing.

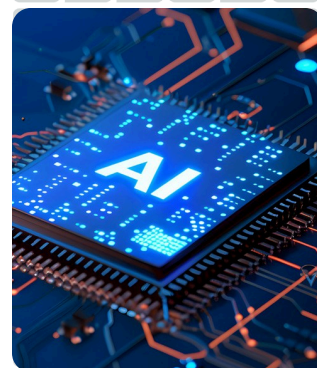
What is it?

"Artificial intelligence (AI) is a set of technologies that enable computers to perform a variety of advanced functions, including the ability to see, understand and translate spoken and written language, analyze data, make recommendations, and more." (Source: [Google Cloud](#))

The same tools that help you write an email or plan a trip help criminals do their jobs faster, cheaper and far more convincingly. AI didn't invent new scams; it supercharged the old ones.

What risk does it solve?

Knowing what these scams look like means you pause before you panic. Every AI scam still needs the same thing the old scams needed: you acting fast, without checking.



What to watch for:

- **The “family emergency” call.** It sounds exactly like your son, daughter or parent. They’re crying; they’ve been in an accident or arrested; they need money now and “please don’t tell Mum.” The voice was cloned from a video they posted. (It may even look like your son on a video call... but it’s a scammer.)
- **The official who isn’t.** A voice message or text from a “government official,” your “bank’s fraud team” or even your “CEO,” asking you to move to WhatsApp, Signal or Telegram. In 2025 the FBI warned that criminals were using AI voices to impersonate senior US officials this way.
- **The celebrity investment tip.** A video of a famous investor or tech CEO promising huge returns on a crypto or trading app. They didn’t say it; AI did.
- **The perfect stranger.** A good-looking profile that messages you, chats for weeks and eventually mentions an “investment opportunity.” The photos and often the conversation are AI generated.
- **The dream job.** A recruiter offers great pay after a quick video interview, then asks for your Social Security number, bank details or a payment for “equipment.” Fake candidates using deepfakes are hitting employers too; it works both ways.
- **The fake explicit photo.** Criminals take normal photos from social media, use AI to make fake nude images and threaten to share them unless paid. This targets teenagers heavily. If it happens: don’t pay, don’t delete the messages, report it at [ic3.gov](https://www.ic3.gov), use [Take It Down](#) to get images of minors removed, and tell a trusted adult.

How to protect yourself:

1. **Set a family safe word. Today.** One of our good friends, Theresa Payton, sat down with me and we talked about AI security. One gem: agree on a “safe word” with your family. Pick a word or phrase that isn’t anywhere online (not a pet’s name, not a street). Agree on it in person, never by text. If anyone calls in a “crisis” asking for money, ask for the safe word. No word, no money.
2. **Hang up and call back.** Use the number you already have saved for that person or the official number on the company’s website.
3. **Slow down.** Urgency is the scam. Real banks, real governments and real family members can wait ten minutes while you check.
4. **Never pay in gift cards, crypto, wire transfers or Zelle** to someone you haven’t verified. Those payments are almost impossible to get back.
5. **Post less audio and video publicly.** Set social profiles to private; the less of your voice and face that’s public, the harder you are to clone.
6. **Test a suspicious video caller.** Ask them to turn their head to the side, wave a hand in front of their face, or answer a question only the real person would know. Live deepfakes still struggle with this.

By the Numbers

In 2025 the FBI logged **22,364** complaints and nearly **\$900 million** in losses where AI was involved.

The FBI says the real figure is far higher; most victims never realize AI was used on them.

Using AI Safely NEW

What is it?

ChatGPT, Gemini, Copilot, Claude, Meta AI... most of us now use at least one AI assistant to write emails, plan trips or answer questions. You may already use AI without noticing, on your phone or

personal assistant devices (aka Siri and Alexa). And some AI tools can now act for you: browse websites, fill in forms and even make purchases.

What risk does it solve?

Whatever you type into an AI tool may be stored, reviewed or used to train future models. And an AI that can act for you can also be tricked into acting for someone else.

How to use:

- **Don't paste in anything you wouldn't post on a billboard.** No Social Security numbers, account numbers, passwords, medical records, photos of your ID or confidential work documents.
- **Check the privacy settings.** Most tools let you switch off "use my data to improve the model" and delete your chat history. Review any "memory" feature so you know what it's remembering about you.
- **Lock down the AI account itself.** It's just another account; use your password manager, a unique password and MFA. Check which apps it's connected to (email, calendar, cloud drive) and remove anything you don't use.
- **Be careful with AI agents and AI browsers.** Tools that browse and click for you can be hijacked by hidden instructions planted on a web page (called "prompt injection"). Even the companies building them say this isn't solved yet. Keep them away from your banking, email and shopping accounts for now.
- **Don't trust an AI for phone numbers or links.** If you need a company's support line, get it from the official website. Scammers plant fake support numbers online hoping AI tools and search results pick them up.
- **Only install official apps.** Download AI apps from the official App Store or Google Play listing by the real company, and AI browser extensions only from trusted sources. Lookalike "AI" apps are a popular way to steal data.
- **Double-check what AI tells you.** AI can be confidently wrong. Don't act on its medical, legal or financial answers without checking a trusted source.

Conclusion:

AI didn't invent new scams; it made the old ones faster, cheaper and far more convincing. The fix is the same as always: pause, verify and never let urgency make the decision for you. Agree on that safe word tonight... it's the cheapest security control you'll ever buy.

NOTE:

As AI evolves we'll keep revising our information and guidance.

Cause everyone's gotta have it in their articles eh... ;-)

Been Scammed? Do This Now

It happens to smart people every day; scammers are professionals. Speed matters more than embarrassment.

1. **Call your bank or card company** using the number on the back of your card. Ask them to stop or reverse the payment and lock the account.
2. **Change your passwords**, starting with your email, and turn on MFA if it wasn't already.
3. **Freeze your credit** at all three bureaus if you shared personal information.

4. **Report it** to the FBI at ic3.gov and the FTC at ReportFraud.ftc.gov. For identity theft, IdentityTheft.gov builds a recovery plan for you.
5. **Watch out for “recovery” scams.** Anyone who contacts you offering to get your money back for a fee is the second wave of the same scam.

Useful Resources

- Want to see if you have compromised accounts? Visit [Have I Been Pwned](https://HaveIBeenPwned.com).
- Dark web monitoring is a service that scans the dark web for sensitive information that may have been leaked or stolen. Many password managers and credit card companies now include it for free; check yours before paying for a separate service.
- Identity theft monitoring: you can also sign up for a service that monitors your accounts and the dark web to guard against identity theft, typically for a fee. If your data is exposed in a breach, the company whose network was breached will often provide one of these services for free for a year or more.
- [FTC Consumer Alerts: learn more about consumer fraud](https://www.ftc.gov/consumer/alerts)
- [FBI’s website for scams and safety](https://www.fbi.gov/scams-safety)
- [FBI Internet Crime Complaint Center \(IC3\)](https://www.fbi.gov/interior/crime-complaint-center)
- [IdentityTheft.gov](https://www.identitytheft.gov)

Credits

Authors: Den Jones & Aaron Wurthmann

Contributors: Tony Bradley

Foreword: Chase Cunningham

Your Protection Checklist **NEW**

Print this page, stick it on the fridge and tick them off. Most take less than 15 minutes.

DO THESE FIRST

- ☐ Freeze my credit at Experian, Equifax and TransUnion (and my kids')
- ☐ Install a password manager and change my most important passwords
- ☐ Turn on MFA for email, banking, phone carrier and social media
- ☐ Agree on a family safe word, in person

ACCOUNTS

- ☐ Switch to passkeys wherever they're offered
- ☐ Set up a separate email address for financial accounts
- ☐ Get an IRS Identity Protection PIN
- ☐ Check my email address at Have I Been Pwned

MONEY

- ☐ Turn on instant transaction alerts for every card and bank account
- ☐ Use Apple Pay, Google Pay or a credit card instead of my debit card

DEVICES

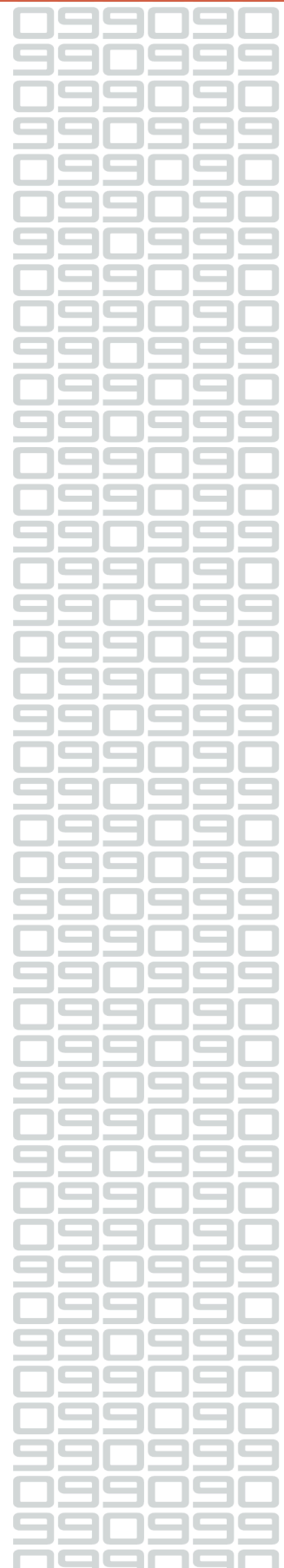
- ☐ Turn on automatic updates on my phone, computer and browser
- ☐ Turn on Stolen Device Protection or Theft Detection Lock
- ☐ Add a PIN and number lock with my mobile carrier
- ☐ Remove browser extensions and apps I don't use
- ☐ Replace or upgrade any Windows 10 computer

SOCIAL MEDIA AND AI

- ☐ Set my social profiles to private
- ☐ Turn off "train on my data" in the AI tools I use
- ☐ Keep AI agents and AI browsers away from banking and email

Remember

Unexpected + urgent + "pay this way" = scam. Hang up, look up the real number, and call back.





909Cyber is a cybersecurity company built on three pillars. **909Shield** is patent-pending hiring fraud detection that verifies the human behind every interview and service desk call, stopping deepfake candidates and account takeover. **909Select** is a freelancer-first US talent marketplace for Cyber, AI, IT and Engineering, powered by 909Shield's identity verification. Our **consultancy** delivers vCISO leadership, compliance, a 24/7 Security Operations Center and security product resale through a "Pragmatic Security" approach that reduces risk and security friction without breaking the budget. Learn more at www.909cyber.com.

© 2026 909Cyber, Inc. All rights reserved.

Second Edition • Last Modified: October 2026