Digital Self Defense Manual (Draft 2_14_24)

```
Start coding or generate with AI.
```

```
Start coding or generate with AI.
```

Digital Citizenship

- **Staying Safe and Responsible when using Digital Technology.**

- **What is Digital Citizenship?**
- **The Components of Digital Citizenship**

What is Digital Citizenship?

- The ability to use technology responsibly, safely and respectfully.
- The ability to protect private information online, mitigate risks associated with cyberthreats or online threats and utilizing information and media in a respectful, knowledgeable and legal way.

The Components of Digital Citizenship

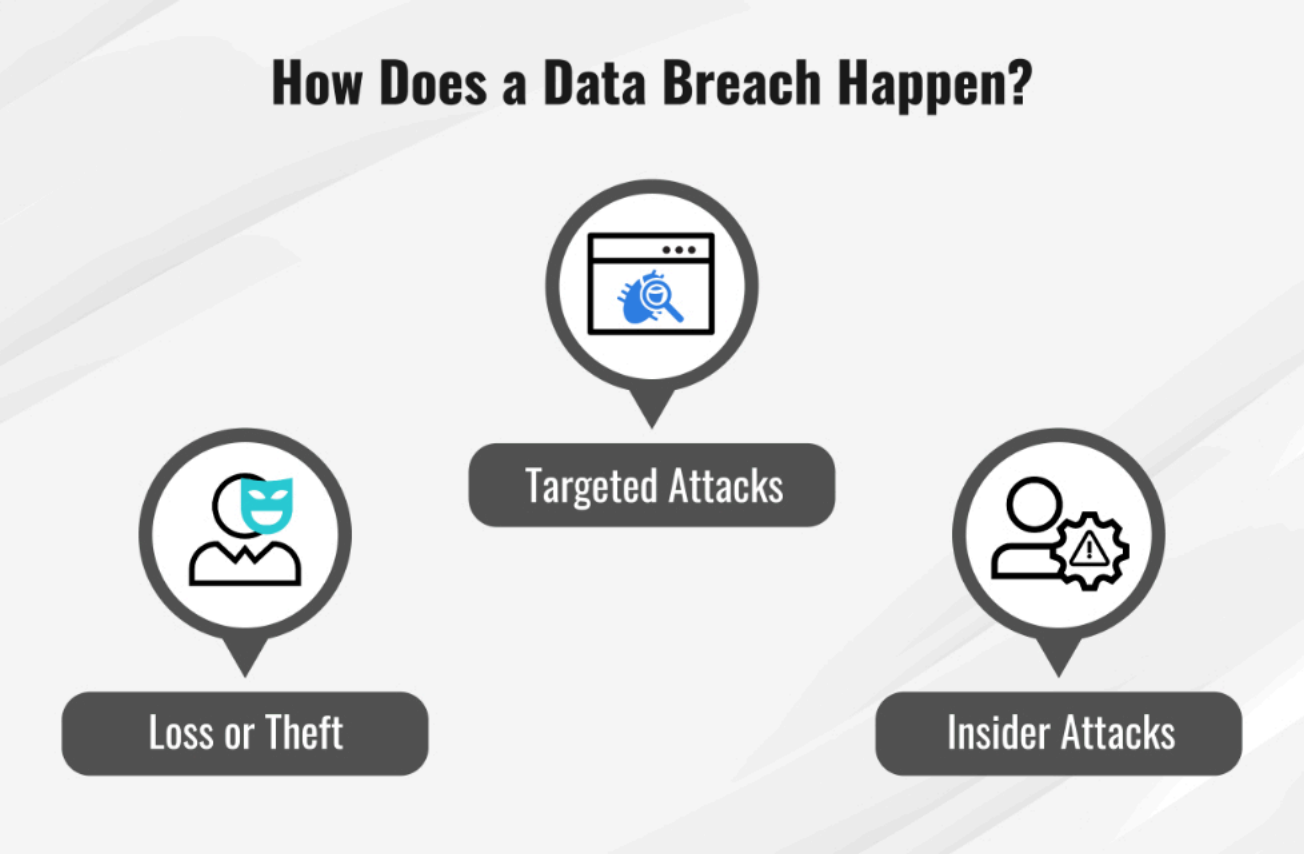
- Online Safety
- Verifying Sources
- Managing Inappropriate Content
- Using Content Responsibly
- Final Thoughts: Teaching Students and Adults Digital Citizenship

Data Breach

- **What is Data Breach?**
- **What is Credit Freeze?**

What is Data Breach?

- Also known as **Data Leakage**.
- A data breach occurs when unauthorized individuals gain access to sensitive, confidential, or protected data.
- This can involve personal information, financial records, passwords, or business data being exposed, stolen, or misused.
- The terms "**data breach**" and "**breach**" are often used interchangeably with "**cyberattack**." However, **not all cyberattacks are data breaches**.



Source

Common Causes of Data Breaches

- **Hacking & Cyberattacks**
  - Criminals exploit vulnerabilities in security systems.
- **Weak Passwords**
  - Easy-to-guess or reused passwords make accounts vulnerable.
- **Phishing Scams**
  - Attackers trick users into revealing login credentials.
- **Malware & Ransomware**
  - Malicious software infects systems and steals data.
- **Insider Threats**
  - Employees or contractors with access misuse or leak data.
- **Lost or Stolen Devices**
  - Laptops, phones, or USB drives containing sensitive data get lost or stolen.

What to Do If You're Affected by a Data Breach

- **Check What Was Exposed**
  - Companies usually notify affected users.
  - Identify if your name, email, passwords, credit card, or Social Security number was leaked.
- **Change Your Passwords**
  - Immediately update affected accounts and use strong, unique passwords. Consider a password manager.
- **Enable Two-Factor Authentication (2FA)**

- Adds an extra security layer for logging in.
- **Monitor Your Accounts**
  - Regularly check bank accounts and credit reports for unauthorized activity.
- **Freeze or Lock Your Credit**
  - Prevents fraudsters from opening accounts in your name.
- **Beware of Phshing Attempts**
  - Scammers might use leaked data to send fake emails or texts. Don't click suspicious links.
- **Use Identity Theft Protection**
  - Services like LifeLock or Credit Karma can alert you to unusual activity.

Notable data breaches

- **TJX**
  - The 2007 breach of TJX Corporation, the parent company of retailers TJ Maxx and Marshalls.
  - As many as 94 million customer records were compromised, and the company suffered more than USD 256 million in financial losses.
  - Hackers gained access to the data by planting traffic sniffers on the wireless networks of two stores.
  - The sniffers allowed the hackers to capture information as it was transmitted from the store's cash registers to back-end systems.
- **Yahoo**
  - In 2013, Yahoo suffered what might be the largest data breach in history.
  - Hackers exploited a weakness in the company's cookie system to access the names, birthdates, email addresses and passwords of all 3 billion Yahoo users.
- **Equifax**
  - In 2017, hackers breached the credit reporting agency Equifax and accessed the personal data of more than 143 million American.
- **SolarWinds**
  - In 2020, Russian threat actors executed a supply chain attack by hacking the software vendor SolarWinds.
  - Hackers used the organization's network monitoring platform, Orion, to covertly distribute malware to SolarWinds' customers.
  - Russian spies gained access to the confidential information of various US government agencies, including the Treasury, Justice and State Departments, that use SolarWinds' services.
- **Colonial Pipeline**
  - In 2021, hackers infected Colonial Pipeline's systems with ransomware, forcing the company to temporarily shut down the pipeline that supplies 45% of the US East Coast's fuel.
  - Hacked by Using employee's password .
  - The Colnial Pipeline Company paid a USD 4.4 million ransom in cryptocurrency, but federal law enforcement recovered roughly USD 2.3 million of that payment.
- **23andMe**
  - In the fall of 2023, hackers stole the data of 6.9 million 23andMe users.
  - The hackers breached user accounts through a technique called "credential stuffing."
  - Disadvantage of reusing the same username and password combinations across sites.

Data breach prevention and mitigation

How to Lock Your Social Security Number (SSN) to Prevent Fraudulent Use

- **Locking or restricting access to your Social Security Number (SSN) can help prevent identity thieves from using it to open fraudulent accounts, obtain employment, or commit other forms of fraud**.

The key ways to lock or protect your SSN

1. **Enroll in the Social Security Administration (SSA) "My Social Security" Account**
    - The Social Security Administration (SSA) offers an online portal where you can monitor your SSN usage.
    - Sign up here: SSA My Social Security / SSN Login
    - Regularly check your earnings record to ensure no one is using your SSN for employment fraud.
2. **Request an SSN Block**
    - You can ask the SSA to block electronic access to your Social Security account.
    - This prevents anyone, including yourself, from making online changes or viewing SSN-related info until you request to remove the block.
    - 📞 Call the SSA at 1-800-772-1213 or visit a local SSA office.
3. **Place a Fraud Alert or Credit Freeze**

- If you're concerned about identity theft, placing a fraud alert or credit freeze prevents criminals from opening accounts in your name.
- ✅ **Fraud Alert**:
    - Notifies creditors to take extra verification steps before issuing credit.
    - Free and lasts one year (renewable).
    - Contact any one of the three credit bureaus to place an alert:
    - Equifax: 1-800-525-6285 or equifax.com
    - Experian: 1-888-397-3742 or experian.com
    - TransUnion: 1-800-680-7289 or transunion.com
- ✅ **Credit Freeze**:
    - Completely locks your credit report, stopping new accounts from being opened.
    - Free and can be lifted anytime.

4. **Enroll in the IRS Identity Protection PIN (IP PIN) Program**
    - If someone has stolen your SSN, they might try to file fake tax returns.
    - The IRS offers an Identity Protection PIN (IP PIN) to prevent fraud.
    - 🔹 Apply here: IRS IP PIN
5. **Monitor Your SSN with Identity Theft Protection Services**
    - If you're worried about SSN misuse, you can subscribe to identity theft protection services like:
    - 🔹 LifeLock, IdentityGuard, or Experian IdentityWorks to receive alerts if your SSN is used fraudulently.
6. **Report SSN Misuse Immediately**
    - If you suspect your SSN is being used fraudulently:
    - 📞 Contact the Federal Trade Commission (FTC) at IdentityTheft.gov
    - 📞 Call the SSA Fraud Hotline at 1-800-269-0271

Steps to Check Your Earnings Record

1. Create or Log in to Your "My Social Security" Account
    - The Social Security Administration (SSA) provides an online portal to view your earnings history.
    - 🔹 Visit: SSA My Social Security Account
    - 🔹 Sign up or log in using a secure username and password.
2. Review Your Earnings Record
    - 🔹 Navigate to "Earnings Record"
    - 🔹 Compare the recorded earnings with your W-2s or tax returns
    - 🔹 If you see extra income that you did not earn, someone else may be using your SSN.
3. Request a Social Security Statement (If You Can't Access Online)
    - If you prefer a paper statement:
    - 📞 Call SSA: 1-800-772-1213
    - 📌 Or fill out Form SSA-7004 to request your earnings statement by mail.
4. Report Any Suspicious Activity
    - If you find incorrect earnings that don't match your work history:
    - 📞 Call the SSA Fraud Hotline at 1-800-269-0271
    - 🔹 Submit a complaint at IdentityTheft.gov

5. Place a Fraud Alert or Credit Freeze (If Identity Theft is Suspected)
   - If someone is using your SSN, protect yourself by:
   - ✅ Placing a fraud alert with credit bureaus (Equifax, Experian, TransUnion).
   - ✅ Freezing your credit to prevent new accounts from being opened in your name.

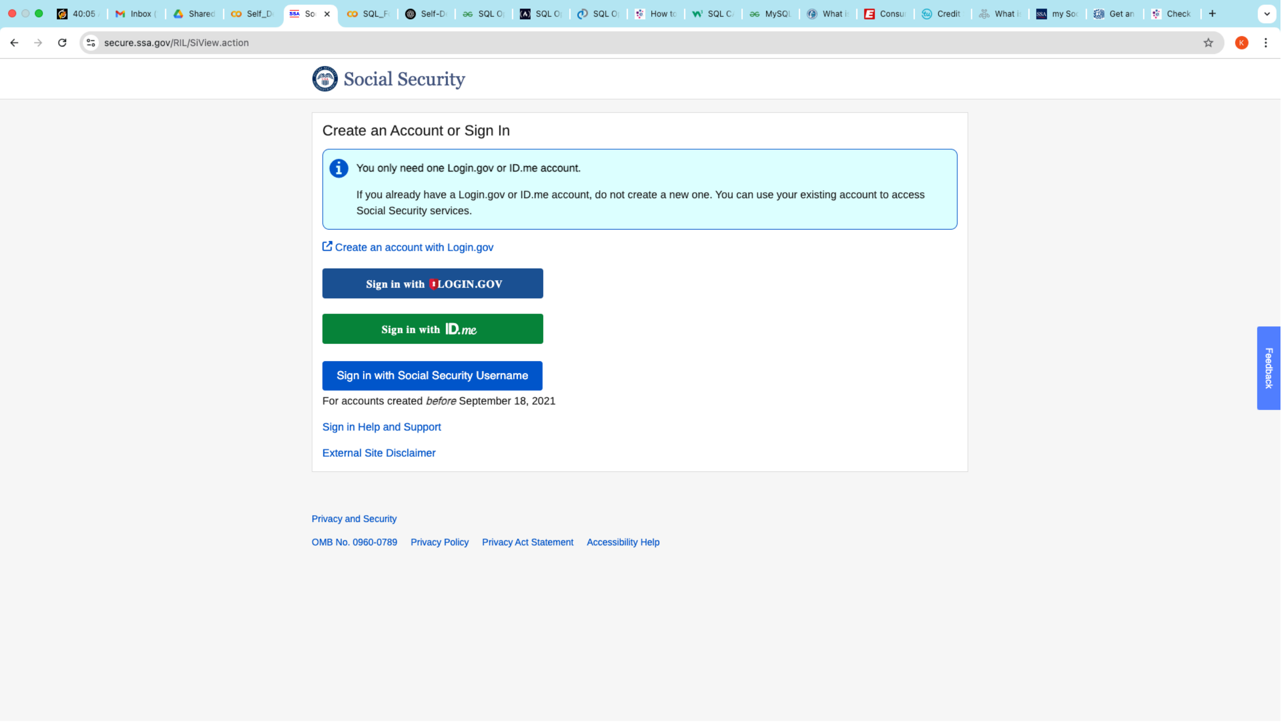
Why Checking Your Earnings Record Matters

- ✔ Ensures you get the correct Social Security benefits when you retire.
- ✔ Detects identity theft before it causes long-term damage.
- ✔ Helps you take action before fraudsters **file taxes or claim benefits** in your name.

How to Claim Your "My Social Security" (mySSA) Account to Prevent Fraud

✅ Step 1: Create Your mySSA Account

- 1️⃣ Go to the Official SSA Website:
- Visit www.ssa.gov/myaccount


secure.ssa.gov/RIL/SiView.action

Social Security

Create an Account or Sign In

You only need one Login.gov or ID.me account.

If you already have a Login.gov or ID.me account, do not create a new one. You can use your existing account to access Social Security services.

Create an account with Login.gov

For accounts created *before* September 18, 2021

Sign in Help and Support

External Site Disclaimer

Privacy and Security

OMB No. 0960-0789 Privacy Policy Privacy Act Statement Accessibility Help

- 2️⃣ **Click "Create an Account"**
- You'll be redirected to the ID.me or Login.gov verification system.
- 3️⃣ **Provide Personal Information:**
  - Full Name
  - Social Security Number (SSN)
  - Date of Birth
  - Mailing Address
  - Email & Phone Number
- 4️⃣ **Verify Your Identity**:
  - SSA will ask you security questions based on your credit history.
  - You may need to upload a photo ID (driver's license, state ID, or passport) for additional verification.
- 5️⃣ Set Up Multi-Factor Authentication (MFA):
  - Choose to receive a one-time code via text, email, or authenticator app for extra security.
- 6️⃣ Create a Strong Password & Confirm Your Account.

✅ **Step 2: Secure Your mySSA Account**

- 🔹 Enable Extra Security Features:
  - Log in and go to "Security Settings"
  - Turn on "Extra Security for Sensitive Transactions"
  - This requires extra verification for future logins.
- 🔹 Block Electronic Access (If Needed):
  - If you suspect fraud, call the SSA at 1-800-772-1213 and request to block electronic access to your SSN.
  - This prevents anyone (including you) from accessing your account online unless you visit an SSA office in person.

✅ **Step 3: Regularly Monitor Your Account**

- ✔ Check your earnings record to ensure no one is using your SSN for employment fraud.
- ✔ Review your Social Security benefits to confirm that no one is falsely claiming them.
- ✔ Update your contact information so SSA can reach you if needed.

✅ **Step 4: Report Any Suspicious Activity**

- 📞 Call SSA Fraud Hotline: 1-800-269-0271
- 📌 Report identity theft at: IdentityTheft.gov

Why Claiming Your mySSA Account Early is Important

- ✔ Prevents identity thieves from creating an account in your name.
- ✔ Ensures you control access to your Social Security benefits.
- ✔ Helps you monitor and protect your SSN from fraud.

How to Put a Freeze on Future Bank Accounts to Prevent Fraud

1. Place a "ChexSystems Security Freeze"

- 🔹 **ChexSystems** is a nationwide banking reporting agency that banks use to verify applicants before opening new accounts.
- 🔹 Placing a security freeze prevents anyone (including you) from opening a new bank account unless you lift the freeze.
- **How to Freeze Your ChexSystems Report**:
  - 1️⃣ Visit: ChexSystems Security Freeze Page
  - 2️⃣ Click: "Place a Security Freeze"
  - 3️⃣ Provide Information:
    - Full Name
    - Address
    - Social Security Number (SSN)
    - Date of Birth
  - 4️⃣ Submit Online or by Mail/Fax
    - 📩 Mail: Chex Systems, Inc., Consumer Relations, P.O. Box 583399, Minneapolis, MN 55458
    - 📠 Fax: 602-659-2197
  - 5️⃣ Receive Confirmation – You'll get a PIN or password to lift the freeze when needed.
    - 📌 Cost: Free
    - 📌 Duration: Until you remove it
  - ChexSystems Consumer Portal Tutorial

2. Freeze Your Reports with Early Warning Services (EWS)

- 🔹 EWS is another banking verification service used by major banks (e.g., Chase, Wells Fargo, Citi) to screen applicants.
- 🔹 A freeze prevents fraudsters from opening new accounts in your name.
- **How to Freeze Your EWS Report**:
  - 📞 Call: 1-800-325-7775
  - 📩 Mail: Early Warning Services, P.O. Box 9201, Scottsdale, AZ 85252-9201

    - 📌 Website: www.earlywarning.com

3. Place a Fraud Alert or Credit Freeze with Credit Bureaus

- Many banks also check your credit report before allowing you to open an account. You can:
    - ✅ Place a Fraud Alert
        - Banks must verify your identity before opening an account.
    - ✅ Freeze Your Credit Report
        - Blocks new credit inquiries entirely.
- 📌 Contact These Credit Bureaus:
    - Equifax: 1-800-525-6285 | www.equifax.com
    - Experian: 1-888-397-3742 | www.experian.com
    - TransUnion: 1-800-680-7289 | www.transunion.com

4. Opt-Out of Pre-Approved Bank Offers

- 🔹 Prevent scammers from intercepting pre-approved banking or credit offers.
- 🔹 Opt-out at: www.optoutprescreen.com

5. Regularly Monitor Your Bank Accounts & Reports

- 🔹 Request a free ChexSystems report once a year to check for suspicious activity.
- 🔹 Sign up for bank alerts to detect unauthorized transactions immediately.

What Happens After You Freeze Your Banking Reports?

- ✔ Banks will deny any new account applications using your identity.
- ✔ You can still use existing bank accounts without issues.
- ✔ You must lift the freeze when you want to open a new account.

How to Place a 1-Year Fraud Alert on Utility Accounts

- If you're concerned about identity theft and want to prevent scammers from opening utility accounts (electricity, water, gas, internet, phone, etc.) in your name, you can place a 1-year fraud alert on your credit file.
- Most utility companies check your credit report before opening a new account, so adding a fraud alert ensures they verify your identity first.

Step 1: Place a 1-Year Fraud Alert with Credit Bureaus

- A 1-year fraud alert notifies utility companies (and other creditors) to take extra verification steps before opening an account in your name.
- 📌 Contact Any One of the Three Major Credit Bureaus (They will notify the other two):
    - ✅ Experian
        - Submit Online | 📞 1-888-EXPERIAN (1-888-397-3742)
    - ✅ Equifax
        - Submit Online | 📞 1-800-525-6285
    - ✅ TransUnion
        - Submit Online | 📞 1-800-680-7289
    - 📌 Cost: Free
    - 📌 Duration: 1 Year (Renewable)

Step 2: Freeze Your Credit Report (Optional but Stronger Protection)

- If you want maximum security, a credit freeze prevents utility companies from accessing your credit file entirely, stopping fraudulent accounts from being opened.
    - 📌 Place a Credit Freeze at Each Bureau:

    - 🔹 Experian: Freeze Here
    - 🔹 Equifax: Freeze Here
    - 🔹 TransUnion: Freeze Here

- 📌 Cost: Free
- 📌 Duration: Until you lift it

Step 3: Contact National Consumer Telecom & Utilities Exchange (NCTUE)

- NCTUE is a member-exclusive Fair Credit Reporting Act (FCRA)-compliant data exchange that compiles telecommunications and utility payment data on millions of consumers.
  - 🔹 Many utility providers check your history with NCTUE, a credit reporting agency for telecom, internet, and utility accounts.
- 🔹 Placing a security freeze on your NCTUE file stops scammers from opening accounts in your name.
- 📌 Freeze Your NCTUE Report:
  - 📞 Call: 1-866-349-5355
  - 🌐 Website: www.nctue.com

Step 4: Monitor Your Utility & Credit Reports

- 📌 Get a Free Credit Report at www.annualcreditreport.com to check for fraudulent accounts.
- 📌 Contact utility companies and ask if any new accounts have been opened in your name.

Step 5: Opt-Out of Utility Pre-Screened Offers

- 🔹 Prevent fraudsters from intercepting pre-approved utility offers in your name.
- 🔹 Opt out at: www.optoutprescreen.com

What Happens After You Place a Fraud Alert?

- ✔ Utility companies will require extra identity verification before opening a new account.
- ✔ You can still open accounts yourself, but they may ask for additional proof of identity.
- ✔ Scammers are blocked from easily using your identity for fraudulent utility services.

How to Add a PIN to Your IRS Account for Extra Security

- **The IRS Identity Protection PIN (IP PIN) is a 6-digit code that prevents scammers from filing fraudulent tax returns using your Social Security Number (SSN).**
- **PIN gives extra layer of security for your tax identity.**

✅ Step 1: Determine If You Are Eligible for an IP PIN

- You can get an IP PIN if:
  - ✔ You were a victim of identity theft or fraud.
  - ✔ You want extra protection even if you haven't been a victim.
  - ✔ You filed a U.S. federal tax return last year.

✅ Step 2: Apply for an IRS Identity Protection PIN (IP PIN)

- 🔹 Option 1: Apply Online (Fastest Method)
  - 1️⃣ Go to the IRS Website:
    - Visit Get an IP PIN
  - 2️⃣ Log in or Create an IRS Account:
    - If you don't have an IRS account, sign up at ID.me
    - You'll need to verify your identity with a photo ID and a selfie.
  - 3️⃣ Complete the Verification Process:
    - Answer security questions to prove your identity.
  - 4️⃣ Receive Your IP PIN Immediately

        - You'll get a new 6-digit IP PIN to use when filing taxes.
- 🔹 Option 2: Apply by Mail (If You Can't Use Online Method)
    - 1️⃣ Complete Form 15227 (IP PIN Request)
        - Download it here: Form 15227
        - You qualify only if your income is below $84,000 (single) or $168,000 (married).
    - 2️⃣ Mail or Fax It to the IRS
        - 📩 Mail: Department of the Treasury, Internal Revenue Service, Austin, TX 73301-0014
        - 🖨️ Fax:855-215-1627 (within the U.S.) Fax: 304-707-9471 (outside the U.S.)
        - Contact-my-local-office-internationally
    - 3️⃣ The IRS Will Call You to Verify Your Identity
    - 4️⃣ Your IP PIN Will Arrive by Mail in 4-6 Weeks
- 🔹 Option 3: In-Person Application (If Identity Verification Fails)
    - 📞 Call the IRS at 1-844-545-5640 to schedule an appointment at a Taxpayer Assistance Center (TAC).Toll free Assistant service : 1-800-908-4490
    - 📌 Bring a government-issued photo ID and SSN card.

✅ Step 3: Use Your IP PIN When Filing Taxes

- Enter your IP PIN on your tax return to prove your identity.
- A new PIN is issued every year, so you must retrieve it before filing.

✅ Step 4: Keep Your IP PIN Secure

- 🔹 Do NOT share it with anyone (except your tax preparer).
- 🔹 If you lose it, retrieve it via IRS Get an IP PIN

- **Why Add an IP PIN?**
    - ✔ Prevents tax fraud using your SSN.
    - ✔ Stops scammers from filing fake tax returns in your name.
    - ✔ Provides an extra layer of security for your IRS account.

Tax Scam:

- **If you get an email, text, letter or call that claims to be from the IRS — or if you see social media posts about how to get a big refund — it might be a scam or bad tax advice.**

Important things to know about an IP PIN

1. It's a six-digit number known only to the taxpayer and the IRS.
2. The program is voluntary, though it’s strongly encouraged.
3. In cases of proven identity theft, taxpayers will be assigned an IP PIN.
4. The IP PIN should be entered on the electronic tax return when prompted by the software product or on a paper return next to the signature line.
5. Only taxpayers who can verify their identity can get an IP PIN.
6. Tax professionals cannot get an IP PIN on behalf of their clients.
7. Each IP PIN is valid for one year. When it expires, a new one is generated for security reasons.
8. Some participants will receive their IP PIN in the mail. Others will have to log in to the Get an IP PIN tool to get their IP PIN.
9. Taxpayers already enrolled in the program can log in to the Get an IP PIN tool to see their current IP PIN.
10. Taxpayers with an IP PIN must use it when filing any federal tax returns during the year, including prior year tax returns or amended returns.
11. IP PIN users should share their number only with the IRS and their tax preparation provider.
12. The IRS will never call, email or text the taxpayer to request their IP PIN.

Types of Cyber Attacks and Their Threats

- 1️⃣ **Phishing Attacks** 🎣
  - 🔹 **What it is**:
    - Fraudulent emails, messages, or websites designed to trick users into revealing personal information, passwords, or financial details.
  - 🔹 **Example**: An email pretending to be from your bank asking you to log in via a fake link.
  - 🔹 **Prevention**:
    - ✅ Verify email sender addresses.
    - ✅ Avoid clicking on suspicious links.
    - ✅ Use multi-factor authentication (MFA) for extra security.

- 2️⃣ **Malware (Viruses, Trojans, Ransomware, Spyware, Worms)** 🦠
  - 🔹 **What it is**: Malicious software that infects your device to steal, damage, or encrypt data.
  - 🔹 **Example**: Ransomware locks your files and demands payment to restore access.
  - 🔹 **Prevention**:
    - ✅ Keep your antivirus software up to date.
    - ✅ Avoid downloading unknown attachments.
    - ✅ Use firewalls to block malicious connections.

- 3️⃣ **Ransomware Attacks** 💰 🔒
  - 🔹 **What it is**:
    - A specific type of malware that encrypts files and demands a ransom for decryption.
  - 🔹 **Example**:
    - The WannaCry ransomware attack locked thousands of hospital and business computers.
  - 🔹 **Prevention**:
    - ✅ Regularly back up data on an external device.
    - ✅ Don’t click on suspicious email links.
    - ✅ Keep software updated to patch vulnerabilities.

- 4️⃣ **Denial-of-Service (DoS) & Distributed Denial-of-Service (DDoS) Attacks** 🌐 💥
  - 🔹 **What it is**:
    - Attackers overload a server, website, or network with traffic to make it unavailable.
  - 🔹 **Example**: Hackers flooding a website with fake requests to crash it.
  - 🔹 **Prevention**:
    - ✅ Use DDoS protection services like Cloudflare.
    - ✅ Implement rate limiting on your website.

5️⃣ **Man-in-the-Middle (MitM) Attacks** 👤🔀👤

- 🔹 **What it is**:
  - Attackers intercept communication between two parties to steal data.
- 🔹 **Example**: A hacker eavesdropping on public Wi-Fi to steal banking credentials.
- 🔹 **Prevention**:
  - ✅ Avoid public Wi-Fi without a VPN.
  - ✅ Use HTTPS websites for secure browsing.
  - ✅ Enable end-to-end encryption for messaging apps.

6️⃣ **SQL Injection (SQLi) Attacks** 💻 📊

- 🔹 **What it is**:
  - Hackers inject malicious SQL code into a website’s database to steal or manipulate data.
- 🔹 **Example**: A hacker gaining access to usernames & passwords from an online store’s database.

- 🔹 **Prevention**:
    - ✅ Use parameterized queries in web applications.
    - ✅ Regularly test for security vulnerabilities.

- 7️⃣ **Credential Stuffing Attacks** 🔑🔒
    - 🔹 **What it is**:
        - Attackers use stolen username-password combos from one breach to access other accounts.
    - 🔹 **Example**:
        - If your password from a leaked website is reused, attackers may access your bank account.
    - 🔹 **Prevention**:
    - ✅ Use unique passwords for every account.
    - ✅ Enable multi-factor authentication (MFA).
    - ✅ Check for leaked passwords on Have I Been Pwned.

8️⃣ **Zero-Day Exploits** 🕵️💣

- 🔹 **What it is**:
    - Attacks that exploit unknown software vulnerabilities before developers release a fix.
- 🔹 **Example**:
    - A hacker discovers a flaw in Windows before Microsoft patches it.
- 🔹 **Prevention**:
    - ✅ Update software as soon as patches are available.
    - ✅ Use intrusion detection systems (IDS) to monitor network activity.

- 9️⃣ **Insider Threats** 🏢🔒
    - 🔹 **What it is**:
        - An employee, contractor, or partner misuses their access for malicious purposes.
    - 🔹 **Example**:
        - A disgruntled employee stealing company secrets.
    - 🔹 **Prevention**:
        - ✅ Restrict access based on need-to-know principles.
        - ✅ Monitor employee behavior & access logs.

- 🔟 **Social Engineering Attacks** 🎭📞
    - 🔹 **What it is**:
        - Hackers manipulate people into revealing confidential information.
    - 🔹 **Example**:
        - A scammer pretends to be IT support to ask for login credentials.
    - 🔹 **Prevention**:
        - ✅ Verify identities before sharing information.
        - ✅ Train employees to recognize phishing & scams.

How to Stay Safe from Cyber Attacks

- 🔒 **Use Strong Passwords**
    - At least 12+ characters with letters, numbers, and symbols.
- 🛡️ **Enable Multi-Factor Authentication (MFA)**
    - Adds an extra layer of security.
- 📲 **Beware of Phishing**

  - Don’t click on unknown links or download attachments.
- 🛰️ **Keep Software Updated**
  - Security patches fix vulnerabilities.
- 🚫 **Limit Personal Information Online**
  - Reduce your risk of identity theft.

How VPNs Can Cause or Contribute to Cyberattacks

- **What is a VPN (Virtual Private Network)?**
  - A VPN (Virtual Private Network) is a security tool that encrypts your internet connection, protecting your online activity from hackers, government surveillance, and even your internet service provider (ISP).
  - It works by routing your internet traffic through a secure server, masking your IP address, and making it appear as if you are browsing from a different location.

- 🔹 **Benefits of Using a VPN**
  - ✅ **Enhanced Security**: Encrypts your internet traffic, protecting you from hackers on public Wi-Fi.
  - ✅ **Online Privacy**: Hides your real IP address, making it harder for websites and advertisers to track you.
  - ✅ **Access Blocked Content**: Bypass geo-restrictions to access websites, streaming services, and apps unavailable in your region.
  - ✅ **Secure Remote Work**: Helps businesses protect sensitive data when employees work remotely.
  - ✅ **Avoid ISP Throttling**: Stops your internet provider from slowing down your speed based on your online activity.

How does VPNs Contribute Cyberattack

- 1️⃣ **Compromised or Malicious VPN Services**
  - 🔹 **Risk**:
    - Some VPNs, especially free or untrustworthy providers, can log user data and sell it to third parties, including hackers.
  - 🔹 **Example**:
    - In 2020, several free VPN services leaked over 1.2 terabytes of sensitive user data, exposing personal information.
  - 🔹 **Prevention**:
    - Always choose a trusted, no-log VPN like NordVPN, ExpressVPN, or ProtonVPN.
- 2️⃣ **VPNs Used by Hackers to Hide Identity**
  - 🔹 **Risk**:
    - Cybercriminals use VPNs to mask their location and identity when launching attacks like phishing, ransomware, and DDoS attacks.
  - 🔹 **Example**:
    - Many ransomware groups use VPNs to connect to victim networks while staying anonymous.
  - 🔹 **Prevention**:
    - Businesses should use network monitoring tools to detect unusual VPN traffic.
- 3️⃣ **VPN Vulnerabilities & Exploits**
  - 🔹 **Risk**:
    - If a VPN has security flaws, hackers can exploit them to breach networks.
  - 🔹 **Example**:
    - In 2021, vulnerabilities in Pulse Secure VPN were used to hack government and corporate networks.
  - 🔹 **Prevention**:
    - Always keep your VPN software updated and use multi-factor authentication (MFA) for VPN logins.
- 4️⃣ **Weak VPN Configurations in Organizations**
  - 🔹 **Risk**:
    - Businesses often use VPNs to allow remote employees to access their networks, but poor security settings can make them an entry point for hackers.

  - 🔹 **Example:**
    - Attackers used a misconfigured Fortinet VPN to access networks and deploy ransomware.
  - 🔹 **Prevention**:
    - Companies should enforce strong authentication, endpoint security, and zero-trust policies.
- 5️⃣ **Free VPNs Injecting Malware**
  - 🔹 **Risk**:
    - Some free VPNs come with malware that can steal your data, track your activity, or display intrusive ads.
  - 🔹 **Example**:
    - HolaVPN was caught selling users' bandwidth and exposing them to cyber threats.
  - 🔹 **Prevention**:
    - Avoid free VPNs and use reputable paid services with a strong privacy policy.

How to Stay Safe When Using a VPN

- ✔ Use a reputable, no-log VPN provider
- ✔ Keep your VPN software updated
- ✔ Enable multi-factor authentication (MFA)
- ✔ Avoid free VPNs that log or sell data
- ✔ Use endpoint security software along with your VPN

How Hard Drives & Thumb Drives Can Be a Cyber Threat

- 1️⃣ **Malware-Injected USB Drives (USB Drops & Attacks)**
  - 🔹 **Risk**:
    - Hackers plant malware-infected USB drives in public places (parking lots, offices, cafes) hoping someone plugs them in.
  - 🔹 **Example**:
    - The “Rubber Ducky” attack uses a USB that acts like a keyboard, executing malicious scripts once inserted.
  - 🔹 **Prevention**:
    - ✔ Never use unknown USB drives.
    - ✔ Disable AutoRun on Windows & Mac.
    - ✔ Use USB security software (like Bitdefender or USB Immunizer).

- 2️⃣ **Ransomware & Data Theft via USB Drives**
  - 🔹 **Risk**:
    - Cybercriminals use USBs to install ransomware on a target’s computer, encrypting data and demanding payment.
  - 🔹 **Example**:
    - In 2022, the FBI warned about USB-based ransomware attacks targeting businesses.
  - 🔹 **Prevention**:
    - ✔ Encrypt your USB drive so even if stolen, data remains locked.
    - ✔ Use only trusted USBs and scan them for viruses.
    - ✔ Keep your OS & security software updated.

- 3️⃣ **Insider Threats & Stolen Data**
  - 🔹 **Risk**:
    - Employees or insiders may copy confidential company files to a USB and leak or sell them.
  - 🔹 **Example**:
    - In 2023, a Tesla employee stole 100GB of data using an external hard drive.
  - 🔹 **Prevention**:

        - ✔ Use Data Loss Prevention (DLP) tools to monitor USB activity.
        - ✔ Disable USB ports on company computers if not needed.
        - ✔ Implement strict access controls & encryption.

- 4️⃣ **Hard Drive Hacking & Data Recovery Attacks**
    - 🔹 **Risk**:
        - If a hard drive is stolen or discarded without being wiped, hackers can recover sensitive data.
    - 🔹 **Example**:
        - Attackers use forensic tools like Autopsy or Recuva to recover deleted files.
    - 🔹 **Prevention**:
        - ✔ Encrypt your hard drive using BitLocker (Windows) or FileVault (Mac).
        - ✔ Physically destroy old hard drives before disposal.
        - ✔ Use secure wiping tools (like DBAN or CCleaner) before selling or recycling drives.

- 5️⃣ **Firmware-Level Attacks on Hard Drives**
    - 🔹 **Risk**:
        - Hackers can infect a hard drive's firmware, making malware persistent even after formatting.
    - 🔹 **Example**:
        - The Equation Group malware (linked to NSA leaks) embedded spyware into hard drive firmware.
    - 🔹 **Prevention**:
        - ✔ Keep firmware updated with manufacturer patches.
        - ✔ Use endpoint protection to detect unauthorized firmware modifications.
        - ✔ Consider self-encrypting drives (SEDs) for extra security.

🔹 **Best Practices to Secure Your Drives** 🔒

- ✅ Encrypt your hard drives & USBs (BitLocker, FileVault, VeraCrypt).
- ✅ Disable USB ports if unnecessary (especially in workplaces).
- ✅ Never plug in unknown USB drives.
- ✅ Physically destroy old or unused hard drives.
- ✅ Regularly scan USBs for malware before opening files.

How to Deny Unnecessary Permissions for Your Phone Apps 📱 🔒

- Many apps request unnecessary permissions that can invade your privacy, drain your battery, and expose you to cyber threats.
- Denying unnecessary permissions helps protect your personal data, location, contacts, and even microphone or camera access from being misused

- 🔹 **Why Should You Deny Unnecessary Permissions?**
    - ✅ **Protects Privacy**
        - Stops apps from accessing sensitive data (location, contacts, messages).
    - ✅ **Prevents Cyber Threats**
        - Reduces the risk of malware and data theft.
    - ✅ **Saves Battery & Data**
        - Prevents apps from running in the background unnecessarily.
    - ✅ **Avoids Spyware Risks**
        - Some malicious apps use permissions to spy on you.

- 🔹 **Common App Permissions to Be Careful About**
    - ✅ Location

        - Some apps track your movements, even when not in use.
    - ✅ Camera & Microphone
        - Apps could secretly record video or audio.
    - ✅ Contacts & Call Logs
        - Apps may collect data on your friends and family.
    - ✅ Storage (Files & Photos)
        - Risk of apps stealing or modifying your files.
    - ✅ SMS & Phone Access
        - Some apps misuse these to send texts or make calls.

🔹 **How to Deny Unnecessary Permissions (Step by Step)** (📱 On Android)

- 1️⃣ Go to Settings > Apps & notifications > App permissions.
- 2️⃣ Select a permission category (e.g., Location, Camera, Contacts).
- 3️⃣ Choose an app and set it to "Deny" or "Ask Every Time".
- 4️⃣ For specific apps, go to Settings > Apps > Select an app > Permissions > Adjust.
- 5️⃣ Disable "Allow Background Activity" if you don't want the app running when not in use.

🔹 **Tip: Android 11+ allows "One-Time Permission" for apps that only need access while in use**.

🍏 **On iPhone (iOS)**

- 1️⃣ Go to Settings > Privacy & Security.
- 2️⃣ Select the permission type (e.g., Location Services, Microphone, Camera).
- 3️⃣ Choose an app and set it to Never, Ask Next Time, or While Using the App.
- 4️⃣ Disable Background App Refresh (Settings > General > Background App Refresh).
- 5️⃣ For microphone and camera, go to Settings > Privacy > Microphone/Camera and toggle off unnecessary access.

🔹 **Tip: iOS 14+ shows orange (microphone) or green (camera) dots when an app is using them**.

Phishing Attacks via Phone Calls

- **A phishing attack via phone call**, often called **vishing (voice phishing)**, involves cybercriminals using phone calls or voicemails to deceive you into revealing sensitive information such as passwords, credit card numbers, or Social Security numbers.

Double-click (or enter) to edit

AI-powered Cyber-Attacks

🔹 **How AI is Used in Cyber-Attacks?**

- 1️⃣ **AI-Powered Phishing Attacks (Deepfake & Voice Spoofing)** 🎭
    - 🔹 **Risk**:
        - AI-generated emails, messages, or phone calls that mimic real people or organizations.
    - 🔹 **Example**: Deepfake voice calls tricking employees into sending money or revealing secrets.
    - 🔹 **Prevention**:
        - ✔ Verify calls & emails before responding.
        - ✔ Use multi-factor authentication (MFA) to prevent unauthorized access.
        - ✔ Train employees to recognize AI-generated phishing attempts.

- 2️⃣ **AI-Driven Malware & Ransomware Attacks** 🦠
    - 🔹 **Risk**:
        - AI adapts malware in real time to bypass security defenses.
    - 🔹 **Example**:

    - AI-powered ransomware that automatically spreads across a network, encrypting data faster than traditional attacks.
  - 🔹 **Prevention**:
    - ✔ Use AI-powered security tools that detect unusual behavior.
    - ✔ Regularly update software & security patches.
    - ✔ Backup your data frequently in a secure location.

- 3️⃣ **Automated Hacking & Password Cracking** 🔒
  - 🔹 **Risk**:
    - AI can guess passwords thousands of times faster than traditional brute-force attacks.
  - 🔹 **Example**:
    - AI-powered bots using machine learning to predict weak passwords and access accounts.
  - 🔹 **Prevention**:
    - ✔ Use strong, unique passwords with a password manager.
    - ✔ Enable multi-factor authentication (MFA).
    - ✔ Monitor login attempts and enable alerts for unusual activity.

- 4️⃣ **AI-Powered Botnets & DDoS Attacks** 🌐
  - 🔹 **Risk**:
    - AI-controlled botnets can coordinate massive cyberattacks to bring down websites and services.
  - 🔹 **Example**:
    - AI-enhanced Distributed Denial of Service (DDoS) attacks that evolve in real time to bypass traditional defenses.
  - 🔹 **Prevention**:
    - ✔ Implement DDoS protection services (Cloudflare, AWS Shield).
    - ✔ Use AI-driven threat detection tools to stop botnet traffic.
    - ✔ Set up network traffic monitoring to detect abnormal patterns.

- 5️⃣ **AI-Powered Social Engineering & Fraud** 📲
  - 🔹 **Risk**:
    - AI analyzes social media & emails to craft ultra-realistic scams.
  - 🔹 **Example**:
    - AI chatbots pretending to be customer service reps to steal credentials.
  - 🔹 Prevention:
    - ✔ Be cautious of unsolicited messages or calls.
    - ✔ Verify customer support contacts on official websites.
    - ✔ Use AI-detection tools to spot fake messages or deepfakes.

- 🔹 How to Protect Against AI-Powered Cyber-Attacks 🔒
  - ✅ Use AI-based cybersecurity solutions to fight AI threats.
  - ✅ Regularly update software to close security gaps.
  - ✅ Enable multi-factor authentication (MFA) to prevent unauthorized access.
  - ✅ Be skeptical of unexpected messages, calls, or emails.
  - ✅ Train employees & individuals on how AI-driven threats work.

References

- https://www.irs.gov/help/tax-scams/recognize-tax-scams-and-fraud
- https://www.experian.com/
- https://www.optoutprescreen.com/
- https://nctue.com/
- https://www.ibm.com/think/topics/data-breach
- https://www.fortinet.com/resources/cyberglossary/data-breach