Tips are designed to reinforce the Agency's Information Security Policy while also drawing upon industry best practices. Check back monthly for new tips on how you can better secure SSA as well as yourself.

January 2025 Tip: Data Privacy - Take Control of Your Data

January 27-31 is Data Privacy Week, sponsored by the National Cybersecurity Alliance (NCA). NCA's goal is to spread awareness of data privacy and teach people behaviors to safeguard their personal and workplace data. Our internet-connected devices and online accounts store Personally Identifiable Information (PII) that needs to be kept secure.

The tips below are important habits to maintain for data privacy at work and at home.

At Work (@ssa.gov)

- All suspected breaches of PII (yours or anyone else's) must be reported to your manager within one hour. The Reporting the Loss of PII website explains the proper reporting procedures.
- Passwords should never be displayed or shared. Any file that contains passwords should be encrypted.
- Keep your HSPD-12 credential (PIV smart card) in your possession or stored securely when not in use.
- If you work with documents that contain PII, keep them secure in a locked file drawer or cabinet when not in use, and destroy them properly when they are no longer needed.
- Only share SSA data with approved partners where the appropriate agreements are in place.
    - Only send PII or other sensitive information to secure email addresses included in the Secure Email Partners List.
    - If you receive an email message intended for someone else, immediately notify the sender and delete the misdirected message.

At Home (Gmail, Yahoo, etc.)

- Protect your accounts by using a unique, complex passphrase for each, and enable Multi-Factor Authentication (MFA) where possible.
- Be mindful of what you share on social media. Birthdates, schools attended, pet names, children's names, mother's maiden names, etc. can be used to guess passwords and answers to security questions, or to give cybercriminals the information to create a false sense of trust with you when trying to lure you into a scam.
- If you must use a public Wi-Fi, use HTTPS websites, use a virtual private network (VPN) if available, and avoid accessing sensitive information such as bank websites or medical office portals.
- Download apps only from trusted sources, avoid third-party apps that are not supported by your device's app store, and delete apps you do not use. There have been many cases where trojan viruses are hidden in apps.
- Keep your software updated. As cybercrime evolves, so do security measures, which are provided by software providers through regular updates and patches.
- If you think someone has accessed your information, you should immediately change the password to that app to prevent additional access.

Resources

Data Privacy Week - National Cybersecurity Alliance

ISP: Section III Protect | OIS

Administrative Instructions Manual System | SSA

Privacy Program

101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Online Safe

Tips are designed to reinforce the Agency's Information Security Policy while also drawing upon industry best practices. Check back monthly for new tips on how you can better secure SSA as well as yourself.

February 2025 Tip: MFA - Because Passwords Aren't Enough

Multi-Factor Authentication (MFA) is one of the most effective ways to safeguard personal and organizational information. MFA adds an extra layer of protection, making it significantly harder for unauthorized users to access accounts, even if they have the username and password. Multi-Factor Authentication is based on the principle that something you know (a password or PIN) is combined with something you have (a physical token, smartphone, or security key) or something you are (biometric data like fingerprints or facial recognition). By requiring multiple forms of verification, MFA strengthens security by ensuring that access is granted only to individuals who can prove their identity in more than one way.

SSA Policy Regarding MFA and Personal Identity Verification (PIV) cards:

- SSA Employees must use their agency issued (HSPD)-12 PIV cards for all (i.e., Windows environments) logical access to agency computers.
- All SSA applications (to include internal applications, as well as IT product/service procurements) must authenticate users through an Agency-approved mechanism, in accordance with:
  - Phishing-resistant multifactor authentication, as established by Enterprise Architecture (Architectural Pattern: Multifactor Authentication (MFA)
  - PIV Interoperability Standards
- In accordance with federal mandates, SSA limits remote access to approved agency solutions with two-factor authentication (e.g., VPN w/PIV cards).

At Home (Gmail, Yahoo, etc.)

- **Activate MFA on Personal Accounts:** Secure your personal accounts—such as email, banking, and social media—by enabling MFA. This reduces the risk of unauthorized access and helps protect personal data from cybercriminals. Email accounts are especially vital because many accounts allow people to reset passwords or use a One Time Passwords (OTP) through email. Unauthorized access to an email account can allow a bad actor to access other accounts that are linked to that email address.
- **Choose the Best Authentication Method for Your Needs:** At home, you have the flexibility to choose the MFA method that best suits your lifestyle. While an authenticator app may be ideal for frequent access, consider using biometric authentication (fingerprint or face recognition) for an added layer of convenience without

compromising security. This article from Tech Republic compares six different authentication apps and explains how they work.

- **Set Up Backup Authentication Options:** Life can be unpredictable—what happens if you lose your phone or can't access your email? Set up backup authentication options, such as backup codes or a secondary device, so you're not locked out of your accounts in an emergency.
- **Avoid Reusing Passwords:** While MFA adds an extra layer of security, it's not foolproof if your password is weak or reused across multiple sites. Always use strong, unique passwords for each of your accounts, and pair them with MFA for maximum security.
- **Enable MFA on Family Devices:** If you share devices or accounts with family members, ensure that MFA is enabled for their accounts too. Whether it's your children's educational tools or your spouse's social media, ensuring that all accounts are protected with MFA strengthens the overall security of your household.

Resources

ISP: Section III Protect | OIS

A Guide to MFA: What It Is, Benefits, and How It Works | PayPal US

What is Multi-Factor Authentication (MFA) and How does it Work? | RSA

Understanding Multi-Factor Authentication | Security Boulevard

6 Best Authenticator Apps | TechRepublic

Tips are designed to reinforce the Agency's Information Security Policy while also drawing upon industry best practices. Check back monthly for new tips on how you can better secure SSA as well as yourself.

March 2025 Tip: Data Backups

Data is one of the most valuable assets we have, yet many people fail to regularly back up their data. This can lead to disastrous consequences in case of a system failure, system hack, or accidental loss. Fortunately, backing up data is simple and can save you from significant loss. World Backup Day on March 31 serves as a reminder to safeguard digital information. This is a great opportunity to evaluate your data backup habits and implement better practices to protect your files.

Data backup refers to the process of copying your important files, documents, photos, and other digital information to a separate storage location. This process ensures that if something happens to the original files (such as a system crash, accidental deletion, or cyberattack), you can recover them without losing everything. There are various methods to back up data, each offering different levels of security, convenience, and cost. The most common methods include cloud backups, external hard drives, and network-attached storage (NAS).

Tips for Backing Up Your Data

- **Follow the 3-2-1 Backup Rule:** The 3-2-1 rule is a best practice for data backup. This means keeping three copies of your data, storing it in two different locations (such as an external drive and cloud storage), and having one copy off-site (e.g., in the cloud). This ensures redundancy and protection in case one backup method fails. (Do not use any personal external storage devices on your SSA-issued device, such as a USB drive. Use of these peripheral devices is a violation of the Information Security Policy (ISP).)
- **Use Cloud Backup for Accessibility:** Cloud services (such as OneDrive, Google Drive, or Dropbox) offer an easy and reliable way to back up your data. Cloud backups are accessible from anywhere with an internet connection and provide protection against local disasters (like a fire or flood) that could destroy physical backups. Microsoft Office documents saved to your online OneDrive allows them to be Auto-Saved, and you can restore previous versions if unwanted changes are made to a file. OneNote is a Microsoft product that saves automatically. It is a great tool for taking notes, organizing documents, and saving emails.
- **Regularly Update Your Backups:** Make sure your backups are up to date. Schedule automatic backups to ensure that your files are always protected. Personal data can be backed up every few weeks or as needed.
- **Encrypt Sensitive Data:** When backing up sensitive information, ensure that the backup is encrypted, especially if you're using a cloud storage service. Encryption protects your data from unauthorized access and ensures that your backup remains secure.
- **Test Your Backups:** Don't just assume that your backups are working—test them periodically. Try restoring a file or folder from your backup to ensure that it is functional and that you can access the data if needed. This simple step can save you time and stress

during a data recovery situation.

- **Hard Copies:** If you must maintain hard copies of documents, keep them securely locked when not in use.

Activity

Go to the World Backup Day website to learn more about why you should back up your data and take the pledge!

Resources

- World Backup Day — Protect Your Data
- DCSI's OneDrive SharePoint site
- M365 Learning Hub
- ISP: Section 3.4.5 System Backup | OIS
- ISP: Section 3.6.3.2 Removable Media Device | OIS
- Backup and Restore in Windows | Microsoft Support
- The Best External Hard Drives for 2024 | PCMag
- Back up your Mac with Time Machine | Apple
- The Best NAS for Most Home Users | NYTimes