Top Ten Things to Do Now to Prevent Identity Theft

1. **Set up a Password Manager and strengthen all of your passwords:** Password managers are secure online vaults that help you create and remember strong and secure passwords, so you don't have to write them down or use simple passwords you can remember for your online activity. Every critical online account - related to banking, email, credit cards, cloud storage, etc. - should have a unique and strong password. A strong password looks like this: **9qK&8*Eo39EmA5@dqTk7aGcrF8**. Of course, there is no way you can remember a password like this, and if you have many of these, one for each high-security online account, you would have a hard time keeping them organized and secure. Password managers alleviate this burden by securely housing all your strong passwords and providing an easy way to update them when necessary. These tools will also work on your mobile device and across most browsers. Some good options are **Keeper, Dashlane, 1Password, LastPass and Bitwarden.**

2. **Set up multifactor authentication (MFA) for your high-security accounts (financial, email, cloud storage, etc.):** MFA, or Multifactor Authentication, verifies your identity by requiring two forms of validation: your password and a PIN code. The PIN code is delivered to your phone either via text/email or generated by an Authenticator App, typically installed on your mobile device.

3. **Freeze Your Credit (same for minors):** A credit freeze limits access to your credit data, protecting you from unauthorized account activities and the fraudulent creation of new accounts in your name. Once your credit is frozen, it can be temporarily lifted to facilitate new credit applications. As of 2018, freezing your credit is free for everyone.

   Below are the credit reporting agencies:
   - Equifax: 800-349-9960 - **www.equifax.com/personal/credit-report-services**
   - TransUnion: 888-909-8872 - **www.transunion.com/credit-freeze**
   - Experian: 888-397-3742 - **www.experian.com/freeze**
   - Innovis: 800-540-2505 **ww.innovis.com/personal/securityfreeze**

4. **Set up automatic software and application updates for all critical software and devices that your use (computer, phone, and tablets):** Most software updates provide critical security

patches that protect your data. Automating these updates, where possible, will save you time and ensure your protection is current.

5. **Set up transaction alerts on all bank and credit card accounts:** Once enabled, your financial institution will notify you via text or email each time a select transaction occurs in your account. Activity alerts are an excellent way to monitor your accounts and detect suspicious activity as soon as it happens.

6. **Sign up for online access and switch to electronic statements for your banking, credit card, and investment services:** Enrolling in online access and transitioning to electronic statements for banking, credit card, and financial services may initially seem counterintuitive to some. However, with robust security protocols—like strong passwords, multi-factor authentication, password managers, and activity alerts, all recommended in this report—online access and electronic statements can arguably offer more security than traditional paper statements. Electronic reports have many advantages, including saving trees, reducing clutter, and preventing thieves from intercepting your mail. If you use electronic access for critical account access and statements, you also should consider establishing a high-security email address.

7. **Establish a unique email address for high-security activities:** Your online access for banking, credit card, financial, and other high-security online accounts all deserve enhanced security. By establishing and using a unique email address for only these accounts, one you do not share or use for any other purposes, you will reduce the spam mail this address receives and reduce exposure to phishing scams commonly associated with junk mail.

8. **Rules for Your High-Security Email Address:**
   - **Dedicated Use:** Reserve this email exclusively for high-security activities.
   - **Secure Access:** Ensure access to this email is limited to secure locations, such as your home or business, and utilize only your computer.
   - **Privacy is Key:** Refrain from sharing, publishing, or forwarding emails from this address, and avoid linking it with any low-security email.
   - **Anonymize the Address:** Choose an email name that doesn't directly associate with you and is challenging to guess. An example might be the names of my last three fictitious dogs (Fido, Spot & Killer) spelled backward: relliktopsodif@gmail.com
   - **Strong Password:** Employ a strong password, ideally generated from a password manager (Refer to #1 on this list).
   - **Routine Password Change:** Update your password is updated regularly.
   - **Use MFA:** Enable multifactor authentication.

8. **Set up verbal passwords for your financial accounts:** Establishing verbal passwords with your bank, credit card, and financial providers adds an extra layer of security when communicating with these institutions by phone.

9. **Utilize an external hard drive or, preferably, a cloud storage service for your important content:** Safeguard and backup your essential documents, photos, and records by storing them on an external hard drive or a cloud storage service. Enable Autosave across all available software to avoid losing important data and content. Some popular cloud services include Google Drive, Apple iCloud, Amazon Drive, Dropbox, and Box. Maintaining regular backups will help protect you and your essential content from ransomware attacks.

10. **Establish your online Social Security account now at www.SSA.gov:** Regardless of whether you're currently receiving benefits, establishing your account with a strong and secure password — is crucial. Each year, identity thieves fraudulently register Social Security accounts and apply for disability or retirement benefits.

Annual Identity Theft Prevention Checklist:

Implementing these annual maintenance activities can provide a solid foundation for protecting your identity and personal information from theft and misuse. Always prioritize securing your digital and physical presence and content by being proactive and vigilant.

1. **Credit report review:** Check and thoroughly review your free annual credit reports from each of the three major credit bureaus (Experian, TransUnion, and Equifax) via www.annualcreditreport.com. Look for any discrepancies or unauthorized accounts and dispute them immediately.

2. **Password management:** Update your passwords quarterly for all critical accounts, such as financial, email and social media, ensuring they are strong and unique. Update all others annually.

3. **Account audits:** Review all financial and payment accounts for any irregularities or unauthorized transactions. Ensure that your contact information is up-to-date on all accounts.

4. **Secure physical documents:** Review, organize, and securely store important documents, such as tax returns, financial statements, insurance policies, estate planning documents, etc. Shred and safely dispose of documents that are no longer needed.

5. **Review beneficiaries:** Ensure that the beneficiaries listed on your financial accounts, insurance policies, and will are current.

6. **Update online, computer and device security:** Verify that the security software on all of your devices is up-to-date (antivirus, antimalware, firewall). Ensure that your devices are updated with the latest security patches.

7. **Register for the Do Not Call registry**: Register your home, office, and mobile phone numbers at https://www.donotcall.gov/register/reg.aspx.

8. **Mail security:** Opt out of pre-screened credit offers via www.optoutprescreen.com or by calling 1-888-5-OPT-OUT. Review your mail regularly and watch out for any missing expected correspondence, which might indicate mail theft.

9. **Secure social media:** Review and update your privacy settings on all social media and online accounts. Be mindful of the information you are sharing publicly.

10. **Mobile service security:** Update all apps and ensure your device's operating system is running the latest version. Review app permissions and revoke any that are unnecessary.

11. **Legal document review:** Revisit legal documents, such as your will and power of attorney, to ensure they remain relevant and accurate.

12. **Educate yourself and family about latest scams:** Stay informed about the latest scams and teach your family members (especially elders and minors) how to recognize and avoid them.

13. **Minimize data sharing:** Review and minimize the amount of personal information shared with organizations and online platforms.