



Take Steps to Prevent Identity Theft with These Tips

Identity theft can be damaging and unsettling. Protecting and safeguarding your financial and personally identifying information is the best way to prevent identity theft and fraud. Act today using the following tips:

Computers

We use computers daily to conduct a myriad of tasks and personal business. Take time to secure your digital accounts with the highest levels of security.

- Make sure your computer has strong anti-virus protection¹
- Install high priority software updates
- Use a long pass phrase including letters, numbers, and symbols for pass words
- Do not use the same password for multiple accounts
- Organize your digital data using a password manager tool²
- Consider adding two-factor authentication.



Be aware of and sensitized to the various types of scams that ask you to supply personal or financial information. For example, be suspicious of emails you don't recognize requesting your information. Do not click on any links in the email and review the email address of the sender. It is often close to something that may be familiar to you, so be extra careful with emails that ask for any personally identifying information. These emails are designed to trick you into providing sensitive information to access your accounts. A popular scam involves email, phone, and texts posing as the IRS. Remember, the IRS will only contact you via the U.S. postal service.

¹ Review U.S. News & World Report's best anti-virus software of 2022 recommendations here. <http://www.usnews.com/360-reviews/privacy/antivirus>

² Recommended password manager tools by C|net, a media website that publishes reviews on technology and consumer electronics. <https://www.cnet.com/tech/services-and-software/best-password-manager/>

Just as you would
review your financial
goals at least annually,
taking steps to
protect your identity
also should be part
of a smart financial
planning checklist.



Mobile Devices

Cyber criminals try to get your personal information using texts with dangerous links within text messages. Do not click on any links in texts you do not recognize. Never provide personal information over the phone to unsolicited callers. Block phone calls you receive that ask for confidential information from any sources you do not recognize. Be careful downloading apps. Make sure they are legitimate and safe. Set up two-factor authentication on your phone and use the same multi-factor authentication for important financial accounts and personal identifying information accounts. Most financial institutions offer top-notch tools and easy-to-follow directions to set up extra security protocols for your phone and computer. Always take advantage of extra security verification measures to protect yourself.


U.S. Mail

Be alert for mail that includes sensitive information and be sure it has been received. This may include credit cards, bank statements, medical bills, or other mail that would be easy for a cybercriminal to obtain your personally identifying information. Pick up your mail daily and make plans to have your mail regularly picked up while you are away. You can also place mail on hold by contacting the U.S. Postal Service. Mail with personally identifying information and other sensitive information should not be tossed in the garbage. Shred any mail containing sensitive information so that it can't be picked out of the garbage and used by a cybercriminal to assume your identity or access your accounts. This is true of ATM receipts tossed in public waste disposal areas. Keep the receipt and shred it later.





Credit Cards and General Theft

Theft of credit cards from businesses with data breaches or unscrupulous employees isn't uncommon and theft of purses or briefcases is one of the leading ways criminals gain access to your credit cards and personal information. Make it a habit to carefully review credit card and bank statements each statement period. You can dispute charges and inform your credit card company and bank of any fraudulent charges. Be aware when you pay for goods and services of how your credit card is being used and by whom. If you use the Internet to shop, be sure the site you are visiting is secure. You can tell if a site is secure if the address is "https" as the "s" stands for secure and look that the site has a lock in front of the address, such as  kayne.com

Should your personal information be part of a data breach, the offending company usually offers free credit monitoring and reports from all the major credit bureaus, so be sure to take advantage of the tools offered to monitor and check your credit.

Play Defense

A good general defense is to check your credit report at least annually. The three major credit agencies – Equifax, Experian, and TransUnion will provide you with a free copy of your credit report. Take advantage of this free review and look for any accounts you did not open, as well as unfamiliar names or addresses. You can request that the credit reporting agencies freeze your credit or place a fraud alert to be attached to your credit report if you find anything suspicious. (Equifax 800-685-1111, Experian 888-397-3742, TransUnion 888-909-8872.)

Protecting your identity provides peace-of-mind and a strong defense against cybercrime. Be vigilant and take steps today to ensure you have the highest levels of security protecting your accounts.



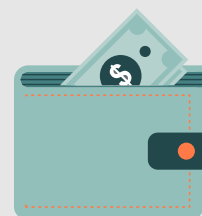
Common Methods of Identity Theft



Cyber Crime



Stealing Mail



**Credit Cards and
General Theft**

Kayne Anderson Rudnick is an investment firm specializing in high-quality investment and wealth management strategies. The firm has an over 30-year history serving a diverse client base that includes high-net-worth individuals, corporations, endowments, foundations, public entities, taft-hartley clients, and mutual funds. Kayne Anderson Rudnick is known for its commitment to high-quality investment strategies and business practices. For more information, please visit www.kayne.com.

This information is being provided by Kayne Anderson Rudnick Investment Management, LLC ("KAR") for illustrative purposes only. Information in this document is not intended by KAR to be interpreted as a recommendation of a particular course of action and has not been updated since the date listed on the article, and KAR does not undertake to update the information presented. KAR makes no warranty as to the accuracy or reliability of the information contained herein. This article provides links to other websites or resources. KAR has no control over such sites and resources, is not responsible for their availability, and does not endorse and is not responsible or liable for any content, advertising, products, or other materials on or available from them. KAR shall not be responsible or liable, directly or indirectly, for any damage or loss caused or alleged to be caused by or in connection with use of such sites or resources. Your use of such sites or resources shall be subject to the terms and conditions set forth by them.