abacus

smart

Security: 10 steps to prevent identity theft

1. Enable two-factor authentication

Two-factor, or two-step, authentication provides an extra layer of security and is highly recommended for all online activity, such as email, online banking, etc. You will need both your password and a one-time code that is sent to your phone to access your accounts.
When enabled, you will login with your current password as usual. In addition, you will be sent a verification code to a trusted phone number via text message or automated call, which you will need to enter to proceed.

2. Review your credit report

You are entitled to one free credit report annually from each of the three major credit reporting bureaus (Experian, Equifax, and Transunion). It is a good idea to compare the credit reports because the information reported may differ among reports. You may request your credit report either directly through the credit bureau's website, by mail and/or phone, or at annualcreditreport.com.
There is a lesser known credit reporting agency: Innovis. Innovis operates much the same as the three main credit reporting bureaus, albeit on a smaller level. Innovis receives information from, and is accessed by, credit grantors related to residential property loans (mortgages), and builds mailing lists, which Innovis sells to creditors. Innovis collects personal identification information such as name, address, date of birth, etc., but does not issue credit scores, and typically does not contain as much information as the larger credit reporting bureaus. You may request a copy of your Innovis credit report through Innovis's website, by mail, or over the phone.

http://www.abacusplanninggroup.com/wp-content/uploads/2015/09/SMARTNOTES_CREDIT-REPORT-A0271263xA7C16.pdf

3. Implement a credit fraud alert, or, even better, a credit freeze. If you already have a freeze, consider updating your PINs.

A fraud alert acts to caution lenders and service providers from granting credit in your name without confirming with you directly. Once you place a fraud alert with one credit bureau, they will notify the others automatically to do likewise. A fraud alert typically lasts only 90 days, although victims of an identity theft can request an extended fraud alert. You must remember to renew at the end of each term to remain protected.

A security freeze prevents any potential creditors from accessing your credit file, and, consequently, prevents any additional lines of credit from being opened. You must establish a credit freeze at each credit bureau which can be done online, via phone, or in writing. You will receive a PIN upon completion, which you would use to temporarily lift (or permanently remove) the credit freeze during specific time periods you plan to apply for credit.

Equifax has recently come under fire for generating non-random PINS (based on date you applied). If you have previously applied for an Experian credit freeze, review your PIN and if necessary, request a replacement PIN.

http://consumersunion.org/research/consumers-unions-guide-to-security-freeze-protection-2/
https://krebsonsecurity.com/2016/01/the-lowdown-on-freezing-your-kids-credit/
https://www.innovis.com/personal/securityFreeze
https://help.equifax.com/s/article/ka137000000DS9XAAW/What-do-I-do-if-I-lose-my-security-freeze-PIN

4. Enroll in a credit monitoring service

Credit monitoring services do not prevent identity theft. What they do, however, is provide an early indication of identity theft (if and when this occurs). These services watch your credit report and alert you if there are any changes, such as new accounts opened in your name, large balance increases, or questionable information. Monitoring services will also help you through the lengthy process of working with creditors and credit bureaus to remove the fraudulent activity from your accounts. These services often also offer identity theft insurance coverage to reimburse associated fees, lost wages, and losses due to identity recovery.

https://www.lifelock.com/products/lifelock-ultimate-plus/
https://www.identityforce.com/products-and-pricing/ultra-secure-credit

5. Opt out of pre-approved credit offers and add your number to the national do-not-call list

Many companies advertising new credit cards, insurance policies, or loans use prescreening to identify potential customers, which is based on information from your credit reports. You may opt out of credit offers for five-year periods by calling toll-free 1-888-5-OPT-OUT (1-888-567-8688) or by visiting www.optoutprescreen.com. You also have the option to opt out permanently, either by requesting online and submitting a signed Permanent Opt-Out Election form, or by sending a written request to each of the major consumer reporting companies.

Adding your name to the National Do Not Call Registry is a free and effective way to reduce telemarketing calls. You may register your phone number online at https://www.donotcall.gov/, or call 1-888-382-1222 from the phone number you want to register.

Security: 10 steps to prevent identity theft

6. Invest in antimalware

Install antimalware on all devices (computer, laptops, tablets, etc.) to monitor, identify, report, and delete any suspicious activity.

Secure your wireless router by adding a password. Be cautious when using free public Wi-Fi; consider using your phone as a hot spot instead.

7. Update your software and back up your information regularly

How many times have you looked at your computer and noticed your software is out of date? Enable automatic updates to ensure your information is constantly protected while eliminating time and effort on your part.

Be proactive about backing up your files to minimize potential damage; if you are hacked, you can quickly and easily restore your data.

8. File your taxes as soon as possible

Tax identity theft can occur when a thief uses your Social Security number to file your tax returns in an attempt to claim a refund. File early to prevent another from attempting to fraudulently file in your name.

Know that the IRS will only contact you via mail. If you receive an email or phone call from "the IRS" requesting information, hang up or delete—it is a scam.

9. Sign up for an online account at the Social Security Administration

Review your existing account (or register for one) to confirm your earnings history is accurate. If you are currently receiving Social Security benefits, confirm the entire amount is appropriately directed into your bank and hasn't been redirected elsewhere.

10. Update your passwords

Regularly update all passwords for email servers, online banking, credit cards, and other online financial accounts. As tempting as it is, never use the same password for two or more websites. Use a password management system, such as LastPass or RoboForm to store, and even generate complex passwords so you only need to know one password to access all your accounts.
Unsure of how to make a strong password? Recent studies show passwords made up of long, meaningful (to you) sentences are stronger even than a string of random letters and numbers. Look at Bruce Schneier's method for inspiration.

11. A bonus tip—Follow Krebs on Security for up-to-date tips

Brian Krebs is a journalist who focuses on cybercriminals. Follow his blog for ongoing and up-to-date security tips.