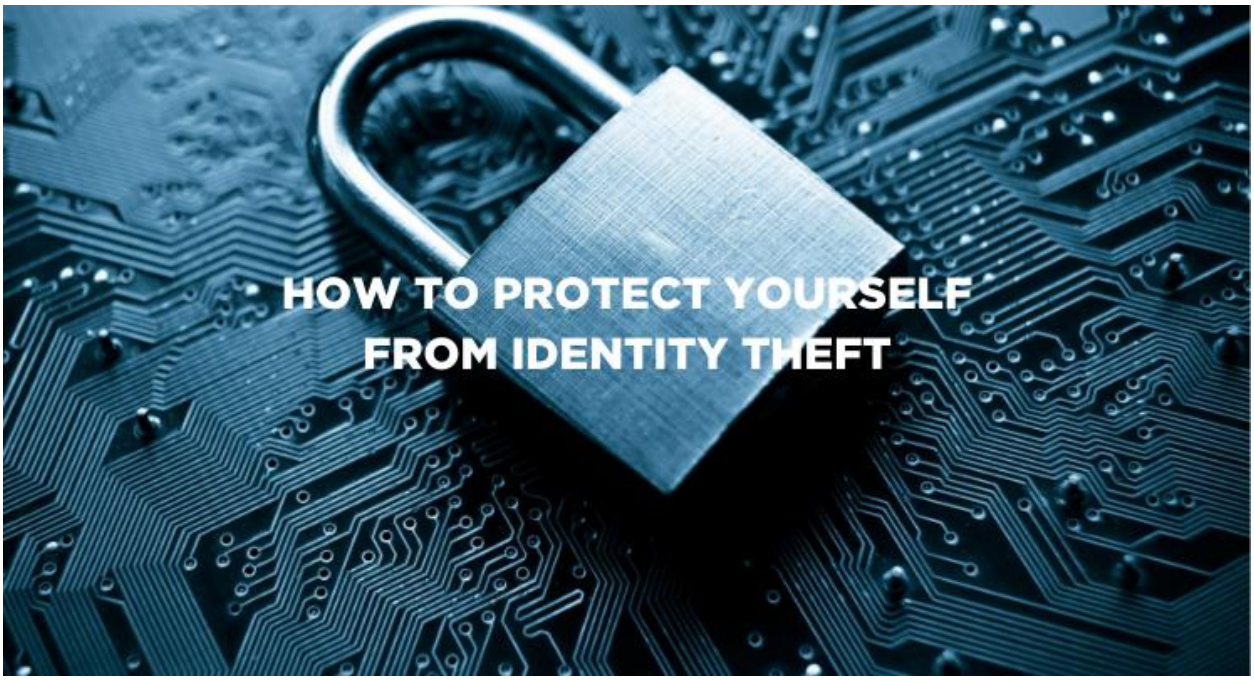

How to Protect Yourself from Identity Theft

Online banking and electronic payment options offer consumers unprecedented access to their financial accounts. Yet, this convenience comes at a price—a greater risk of identity theft. Identity thieves can use your personal information to open fraudulent accounts and steal your money through unauthorized purchases and withdrawals. Luckily, there are steps you can take to protect against identity theft and reduce the damage when it happens.

Check your credit report and account statements

If fraudulent transactions are draining your account balances or new accounts are being opened in your name, it is important to know as soon as possible. Check your banking statements regularly—at least once a month, but as frequently as every week—for purchases, withdrawals or transfers you do not recognize. Also check your credit report for suspicious activity. Each of the three major credit bureaus—Equifax, Experian, and TransUnion—let you access your credit report for free once a year. By staggering your reviews from each bureau, you can get a copy of your credit report every four months.

Set up safeguards with your bank

Your bank, credit union or credit card issuer likely offers its own fraud protection, such as notifications of suspicious activity or a system that disables your credit card after an unusual purchase. Contact your financial institution to learn more about the options available to you and what you need to do to implement them.

Use privacy software

Install antivirus software on your computer to prevent hackers from retrieving personal data on your hard drive that could be used to access your accounts. Keep your operating systems, browsers, and financial apps up to date so you can be sure you have the latest security features. Store your passwords in dedicated password management software, never in your web browser, which typically has too many vulnerabilities to keep your passwords secure.

Practice good password management

In addition to using the right software to store your passwords, there are several things you should do to practice good password management:

- Update your passwords every month.
- Assign a different password to each login.
- Choose long passwords that mix numbers, letters, and special characters, and are not based on your personal information.

You may also consider keeping unique, frequently updated password on a list of paper. While some IT experts frown upon the idea of writing passwords down, keeping a hard copy list can be appropriate for accounts you only ever access at home, especially if it makes it possible for you to maintain stronger passwords.

Recognize phishing scams

All the encryption in the world will not protect you if you unwittingly divulge your password to an identity thief. Learn to guard against phishing scams—messages designed to trick you into revealing your personal information by posing as a legitimate entity.

Be skeptical of emails that purport to be from corporations or government agencies that urge you to “confirm” your personal information or password by clicking on a link from within the email. When in doubt, contact the entity through a trusted email address or telephone number to ask whether the message is legitimate.

You can limit the damage from having your passwords phished by setting your online accounts for two-factor authentication, which requires an additional piece of information to log in.

Report fraudulent activity immediately

The sooner you inform your financial institutions of breached accounts or stolen information, the easier it will be to minimize the loss. If you lose your credit or debit cards, call your bank to cancel them and request replacements immediately. If the account itself is hacked, your bank can close it. If you suspect that your password has been phished, change your password, and contact the bank that keeps the account.

If you believe someone has stolen your Social Security number:

- Contact the Social Security Administration.
- Contact the Federal Trade Commission to file a complaint.
- Contact every financial institution where you have an account.
- Contact the Equifax, Experian and TransUnion to request a fraud alert to prompt potential lenders to or credit freeze to prevent lenders from accessing your credit report and therefore prevent an identity thief from opening an account, renting an apartment or applying for a loan in your name.

It takes effort and vigilance to keep your personal information safe but doing so can help minimize the potential of having your financial life upended by fraud or identity theft.

Sources:

https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams
https://www.experian.com/blogs/ask-experian/3-steps-to-take-if-your-social-security-number-has-been-stolen/
https://www.equifax.com/personal/education/identity-theft/what-to-do-if-you-lose-your-social-security-card/
https://www.howtogeek.com/howto/31259/ask-how-to-geek-what%E2%80%99s-wrong-with-writing-down-your-password/

Disclosures:

This information has been obtained from sources considered to be reliable, but we do not guarantee that the foregoing material is accurate or complete. Any information is not a complete summary or statement of all available data necessary for making an investment decision and does not constitute a recommendation. This material was created by The Oechsli Institute, an independent third party that is not affiliated with Balance Wealth.

This Presentation was created for educational and informational purposes only and is not intended as ERISA, tax, legal or investment advice. If you are seeking investment advice specific to your needs, such advice services must be obtained on your own separate from this educational presentation.

Securities offered through LPL Financial, member FINRA/SIPC. Investment Advice offered through Independent Advisor Alliance, a registered investment advisor. Independent Advisor Alliance and Balance Wealth Partners are separate entities from LPL Financial.