Identity theft is one of the most common cybercrimes, which involves cyber criminals stealing someone’s critical information such as name, telephone number, address, bank account details, credit card numbers or Social Security number. This information is then used by scammers to work in different ways such as applying for loans or credit cards, setting up cell phone services, opening bank accounts, doing online shopping, or opening bank accounts.

Avoiding identity theft depends on how vigilant you are while dealing with your sensitive data. Below are 10 ways that can help you prevent identity theft and safeguard your personal information.

1. **Freeze Your Credit Report**

Freezing your credit file prevents anyone, including you, from viewing your credit report. Thus, no one can open an account, get a new credit card, or apply for a loan when your credit is frozen. To do this, you need to contact the credit reporting agencies, i.e., Equifax, Experian, and TransUnion by through online, main-in, or telephone option. They provide a passcode or PIN in case you want unfreeze your credit. Credit freeze is a free facility and does not impact the credit score of the [card holder](http://www.cardzgroup.com/ContactLessSmartCard.html).

1. **Collect Your Mail Everyday**

This is a simple and relatively easy way for criminals to get hold of your personal data. It is important for you to collect your mail daily from the mailbox, as criminals can easily take utility bills, credit card statements, tax or healthcare forms from it. It is also important to keep track of expected mail that does not arrive, as these criminals can also reroute your mail to their own address by requesting change of address.

1. **Regularly Review Bank Account and Credit Card Statements**

This is particularly important to ensure that no one is using your credit card or account details to make small and insignificant transactions that can often go unnoticed. It is important to know your statement cycle. If you don’t receive your statements on time, always follow up with your financial institution or credit card company.

1. **Always Shred your Personal Documents before Disposing them Off**

With all the online data breaches and phishing scams going on, dumpster diving may seem like an old method of stealing critical information. However, many criminals still do it. Therefore, it is important to always shred your bank and credit card statements, utility bills, and other sensitive documents before disposing them off. You should also keep your recent statements in a secure location, in case you might need them in near future.

1. **Keep Different Passwords for Different Accounts**

This is specifically important because if criminals are somehow able to breach one of your accounts, they should still be unable to hack into your other accounts. If you keep the same password for all accounts, it is very likely that all your accounts will get hacked. The easiest way to keep different passwords is to use a good password manager. It is also important to follow best practices for keeping a password. Also avoid using your personal information in your passwords, such as your birthday, name, or Social Security number.

1. **Review Your Credit Reports Once a Year**

It is free to request your credit reports from Experian, Equifax, and TransUnion and it does not lower your credit score. Hence, you must review your reports annually. The credit bureaus also provide tools that help cardholders to monitor their credit, such as alerts notifying of key changes.

1. **Install Antivirus Software on your Device**

Antivirus can prevent cyber criminals from accessing critical information on your mobile devices and computer. If your device slows down, fails to restart or shut down, displays error messages, drains its battery quickly, changes your default web browser, etc., it may indicate that you are a victim of malware. It is also important to keep your antivirus software updated, since criminals can easily hack it if it’s outdated.

1. **Enable Two-Factor Authentication on your Accounts and Devices**

Even with strong passwords in place, criminals can still hack into your account. Two-factor authentication adds an extra layer of authentication besides password, which makes it difficult for cyber criminals to breach your account. Even if your password is stolen, they can still not access your account unless they are able to authenticate it with a second factor. Two-factor authentication or 2FA can be enabled for social media accounts, email, credit cards, and bank accounts. It can include combinations of a password along with a PIN code, biometric characteristic, or a smartphone authentication.

1. **Wipe out Data from Electronics Before Selling or Donating**

When deleting data files from your computer or other electronic devices, some parts of the data still remain. Hackers can reassemble the data by using a data recovery program. Thus, when you are selling or donating your device, it important to completely wipe out your data by using an overwriting or data shredding software.

1. **Unsubscribe to Prescreened Credit Card Offers**

Cardholders often get prescreened offers from credit card companies to open new accounts. Criminals intercept and use these offers to open an account in your name. The best way to avoid these offers is to opt out of getting them in your mail or email.

**What to do if you are a Victim of Identity Theft?**

If you fall victim to identity theft, you need to block your bank account and credit cards. It is also advisable to report the theft to the police if you are aware of who committed the crime, or if they used your identity during a police interaction.