



# Tips to Minimize Your Risk of Identity Theft



Identity theft continues to increase, but you can minimize your risk by managing your personal information smartly and safely.

## Create unique passwords out of a random mix of letters, numbers, and special characters.

Complex, unique passwords make it harder for identity thieves to gain access to your online accounts. You should also change all of your passwords on a regular basis.

## Don't overshare online and be wary of email scams.

- Don't post any personally identifiable information (PII) about yourself online.
- Be aware of suspicious "phishing" email scams, and never send information such as your Social Security number (SSN), credit card number, or User ID/Password through an email.

## Use the latest anti-virus software and be careful with public WiFi networks.

- Update your computer and devices with the latest anti-virus software to help protect against harmful malware and viruses.
- Try to avoid using public WiFi networks or hotspots, as these can be an easy way for criminals to steal your personal information. If you must share personal information online for transactions, make sure you are using a secure network.

## Only carry essential documents and cards with you.

Avoid carrying extra credit and debit cards, your Social Security card, your birth certificate or your passport with you outside the house, and keep these items secured.

## Check your credit report at least every 12 months.

The three nationwide credit reporting bureaus have set up a central website through which you can order your free annual credit report. Visit [www.annualcreditreport.com](http://www.annualcreditreport.com) to request a free copy of your credit report every 12 months from each bureau. Check your report for signs of suspicious activity, such as unfamiliar accounts. You should also strongly consider subscribing to a credit monitoring service.

## Protect your Social Security number at all times.

Only a few organizations, such as motor vehicle departments, tax departments and welfare departments, have the right to require your SSN. In addition, employers, banks and other financial institutions sometimes require your SSN for tax purposes. For all other instances, you should ask if you can provide an alternative proof of identification.

## Be cautious when giving out personal information over the phone.

- Identity thieves may call you, posing as banks or government agencies. Do not give out personal information over the phone unless you initiated the call.
- Register your phone number with the National Do Not Call Registry to avoid calls from telemarketers trying to get your information over the phone. Visit [www.donotcall.gov](http://www.donotcall.gov) for more information.

## Make sure others are keeping your information safe.

- Ensure that your employer, landlord, medical care facilities and anyone else with access to your personal information keeps your records safe.
- Be sure to read any privacy policies if you must share information with outside entities.

## Shred your sensitive documents.

Before discarding items containing PII, shred them. This includes items such as receipts, bank statements, and returned checks.

## Stay on top of your billing cycles.

Making sure you receive your credit card bill every month is an easy way to help prevent identity theft. Whenever it's available, you can also request online billing, which is more consistent and easier to track than regular mail.

## Keep the fraud department contact information handy.

In the event of identity theft, it's important that you alert your banks and creditors quickly in order to avoid or reduce your losses. Each of your accounts should have its own fraud department; have those numbers readily available if you ever need them.

## Keep your new checks out of the mail.

Pick up your checks at the bank instead of having them sent to your home when you order new ones. This makes it harder for your checks to be stolen, altered and cashed by identity thieves. Additionally, remove any unnecessary private information (e.g., driver's license number) from your checks.

## Give your mailbox a makeover.

Every pre-approved offer you receive in the mail is an invitation for someone to open a credit line in your name, so limit the amount of junk mail you receive. Contact the Direct Marketing Association's Mail Preference Service to opt-out of these offers.

- **Online:** Visit and register at [www.dmachoice.org](http://www.dmachoice.org)
- **By mail:** [Download this form](#)<sup>1</sup> and send a \$1 check or money order payable to the DMA at:

DMA Choice  
Direct Marketing Association  
PO Box 643  
Carmel, NY 10512

**Following these easy tips will help safeguard your identity.**

<sup>1</sup> [https://www.dmachoice.org/static/pdf/registration\\_form.pdf](https://www.dmachoice.org/static/pdf/registration_form.pdf)