9 Tips to Protecting Yourself from Identity Theft

Presented by Jessica DiMatteo

Like many people, you might believe that your identity could never be stolen. Then, one day, you go to the mailbox, open your monthly credit card statement, and see a host of charges made to your account in a country you've never visited. Millions of Americans fall victim to this type of identity theft every year.

Given that identity theft is so prevalent, what can you do to safeguard yourself and your family? While we can't guarantee these tips will keep your personal information safe from fraudsters, we can recommend several best practices that are worth implementing.

Be aware of potential impersonators. Don't give out personal information over the phone unless you're the one who initiates contact or you're absolutely certain about with whom you are speaking. If a caller requests personal information, hang up, look up the phone number of the business the caller claims to represent, and dial the number to verify the caller's identity.

The same advice applies to any suspicious emails you receive. Verify who is sending the message by calling the organization that supposedly sent the email, and **don't click on any links or attachments that come with the message**.

Safely dispose of personal information. Before you discard a computer, back up your data and delete all the personal information on it. Deleting is not sufficient protection, however, so it's best to also use a program meant for wiping or overwriting the entire hard drive. Also, consider removing the hard drive and having it securely destroyed. To do this, you can either break the circuit board in half, or use a certified data disposal service and ask for a certificate of destruction.

Before disposing of a mobile device, transfer the contents you want to retain and then permanently wipe the device. Instructions for a data wipe of your specific device can be found via an online search. Be sure to remove the memory and SIM card before recycling, selling, or giving the device away.

You'll also want to shred documents you no longer use. Old credit cards, bank statements, and cash advance applications should all be destroyed.

Encrypt your data. Encryption prevents unauthorized access to digital software. In addition to installing encryption software to protect your laptop in case it's lost or stolen, keep your browser secure by looking in the address bar for a lock symbol. When it appears, it means your information is being securely transmitted. In addition: *Never* make credit card purchases on unsecured websites whose addresses begin with the letters HTTP. *Always* look for secure sites, which begin with "HTTPS."

Keep passwords private. Use strong passwords—at least 12 characters long and combinations of upper- and lowercase letters, numerals, and symbols—and be sure you use a different one for each account. Don't use personal information or words found in the dictionary and consider using a password manager to autogenerate and store your passwords.

Don't overshare on social media. The more personal information you post about yourself, your family, and your children, the easier it is for criminals to potentially guess your security questions. They may even be able to figure out where you live and when you are home. In addition to using your account settings to limit who can view your posts and photos, keep the following tips in mind: *Never* accept requests from people you haven't met or don't know personally; they could simply be posing as a friend. *Never* post your full name, address, social security number (SSN), account numbers, names of your children, and addresses on public websites.

Read privacy policies. These policies tell you how the site or company with which you're doing business maintains the information you share, and what is collected and stored. The policies also explain how the company uses the information, who accesses stored information, and whether it is provided to third parties. If you don't see or understand a site's privacy policy, consider doing business elsewhere.

Secure your SSN. Before sharing your SSN, ask questions about why a vendor or organization needs it, how it will be used, how it is protected, and what happens if you decline to give it out.

Check your credit. The Fair and Accurate Credit Transactions Act requires the three major credit monitoring agencies (Equifax, Experian, and TransUnion) to offer consumers a free report once per year. This means that you can conduct a credit check every four months. We recommend performing a *minimum* of three credit checks each year to make sure all the information is correct, you are familiar with all open accounts, and verify all entries in the inquiries section

There are numerous companies around that will monitor your credit, your accounts, the Internet, and social media for suspicious or criminal activity. These companies will alert you about changes to your credit—one of the first signs of identity theft. For additional fees, they will also monitor your children's SSNs.

These are only a few tips to help keep your identity safe. For a host of options, visit the Federal Trade Commission website. And if you ever fall victim to identity theft—or suspect you may be a victim—check out identitytheft.gov for valuable guidance and resources for your specific situation.

We're always concerned about information security, and we strive to keep you updated on new security threats, as well as potential solutions to help protect your information. If you have any questions, please contact our office by phone or email.

DiMatteo Group
FINANCIAL SERVICES

Jessica DiMatteo
DiMatteo Group Financial Services Inc.
1000 Bridgeport Avenue | Suite 506 | Shelton, CT 06484
203.924.5420 | 203.402.8305 fax | www.dimatteofinancial.com | jessica@dimatteofinancial.com