

9 TIPS

PROTECTING YOURSELF FROM IDENTITY THEFT

You may be like most people. You believe that identity theft could never happen to you. 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 dreamed of visiting. That's a type of identity theft, and you've become one of the millions of its victims in the U.S. every year.

What can you do to protect yourself?

Given that identity theft is so prevalent, what can you do to safeguard yourself and your family? Certainly, there are no guarantees, but we can recommend several best practices that are worth implementing.

- 1. Be alert to impersonators.** Don't give out personal information over the phone unless you initiate the contact or are absolutely certain with whom you are speaking. If a caller requests personal information, feel free to 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.

Same goes for any suspicious e-mails you receive. Verify who is sending the message by calling the organization that supposedly sent the e-mail, and **don't click on any links or attachments that come with the message.**

- 2. Learn how to safely dispose of personal information.** Before you dispose of a computer, get rid of all the personal information on it and use a program to wipe or overwrite the entire hard drive. Also, consider removing the hard drive and having it securely destroyed.

Before disposing of a mobile device, transfer the contents you want to retain and then permanently wipe the device. And be sure to remove the memory and SIM card before recycling, selling, or giving the device away.

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

- 3. Encrypt your data.** 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.

- 4. Keep passwords private.** Use strong passwords—at least eight 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.
- 5. 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.
- 6. Read privacy policies.** These policies tell you how the site or company you're doing business with 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.
- 7. 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.
- 8. Take advantage of FACTA.** 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.
- 9. Get credit monitoring for yourself and your family.** 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.

Rest assured that we are always concerned about information security, and we will strive to keep you up to date on new security threats, as well as potential solutions to help protect your information. If you have any questions, please contact us at 210.495.8474 or toll-free at 888.757.2104.



BusinessFinancialGroup.com

210-495-8474 / 1-888-757-2104

Business Financial Group provides corporate services, including human resources consulting, compliance and administration support, payroll and employee benefit program development and maintenance. We also provide group retirement and personal financial planning services.

Securities and advisory services offered through Commonwealth Financial Network®, Member FINRA/SIPC, a Registered Investment Adviser. Human resources services and consulting, payroll processing services, employee program development and maintenance services, fixed insurance products and services offered by Business Financial Group are separate and unrelated to Commonwealth. Business Financial Group is located at 500 North Loop 1604 East, Suite 250, San Antonio, Texas 78232.

This material has been provided for general informational purposes only and does not constitute either tax or legal advice. Although we go to great lengths to make sure our information is accurate and useful, we recommend you consult a tax preparer, professional tax advisor, or lawyer.