Call us:
800.545.4442

Email us:
info@towneley.com

Visit us online:
www.towneley.com

AUGUST 17, 2021

PROTECT YOURSELF FROM IDENTITY THEFT AND CYBERCRIME (3-PART SERIES)

PART 1: PREVENTING IDENTITY THEFT

THIS PAPER IS PART 1 of a 3-part series on protecting yourself and your loved ones from identity theft and cybercrime.

- PART 1 outlines some steps you can take to protect your identity.
- PART 2 focuses on protecting your computer from cybercriminals.
- PART 3 identifies clever tricks and scams to avoid.

Welcome to 2021 — the 21st Century. Today, we have more technology at our disposal than ever before, making our lives easier and more enjoyable. We can bank in a bathrobe from the comfort of our kitchen and connect with friends and loved ones around the globe anytime, day or night. In addition, we can conduct business meetings, complete with visual aids, without being in the office (thanks, COVID-19!). Yet, with all the perks and ease that modern-day technology brings to our lives, unfortunately, it has also made it easier for cybercriminals to access our private information.

However, don't despair — the good news is that there are several steps you can take to protect your personal information and keep your private data private in this modern, digital world.

Here Are Six Things Cyberthieves Can Do With Your Personal Information – And Several Things You Can Do To Stay Safe

1 **Open credit card accounts and bank accounts, and take out loans, in your name.** A defrauder who gets ahold of your social security number can do significant damage, such as applying for government benefits, opening bank and credit card accounts, applying for a loan or utility service, or even renting a place to live in your name. Because of this, you should not provide your social security number to anyone unless there is a legitimate reason, such as applying for employment, opening a financial account, or financing a large purchase. It's also good practice to never carry your social security card with you in case your wallet or purse is misplaced or stolen. The same goes for your kids' social security cards, too – all should be kept in a safe deposit box, a personal fire safe, or at the very least, a good hiding spot in your home.

But even those of us who are most diligent about protecting our private information are still subject to things out of our control. With the number of massive data breaches and cyberattacks in recent years, let's face it – all of our social security numbers are floating through cyberspace at this point. Thankfully, you can take some additional steps to help protect yourself from this version of thievery.

First, check your credit reports periodically for unusual activity or new accounts that you didn't open. There are four credit reporting bureaus, and you are allowed to check each report once per year at no charge and without affecting your credit score. To order your Experian, Equifax, and TransUnion credit reports, go to annualcreditreport.com. To order your Innovis credit report, go to innovis.com/personal/creditReport.

Second, it's a good idea to freeze all four of your credit files. A credit freeze restricts access to your credit reports by current and prospective creditors. Once your credit file is frozen, you and only you can unfreeze it. A wise practice is to keep your credit files frozen until it's time for you to obtain new credit, say, next time you want to lease a car or refinance your mortgage. If you do freeze your credit files, you'll want to keep the PIN created during the freezing process (each credit bureau will issue a unique PIN to you) – you will need the PIN to unfreeze your credit file. Federal law also allows you to freeze your minor children's credit files to protect their information. You can freeze your credit files by mail, phone, or online, but it's easiest to do it online.

Here's the contact information for freezing your credit with each of the four credit agencies:

Experian: (888) 397-3742
P.O. Box 9554 Allen, TX 75013
experian.com/freeze

TransUnion: (833) 395-6938
P.O. Box 2000 Chester, PA 19016
transunion.com/credit-freeze

Equifax: (888) 298-0045
P.O. Box 105788 Atlanta, GA 30348
equifax.com/personal/credit-report-services

Innovis: (800) 540-2505
P.O. Box 26 Pittsburgh, PA 15230
innovis.com/personal/securityFreeze

Additionally, identity thieves are not above digging through trash bins to find your sensitive information! Protect written information by shredding sensitive documents (bank statements, credit card offers, etc.) with a cross-cut, micro-cut or diamond-cut shredder to foil this tactic. Also, don't leave outgoing mail with personal information in an unlocked mailbox for pickup, especially outgoing mail enclosing a handwritten check for a bill payment. If a thief gets that valuable piece of mail, he now has your bank account number, routing number, account name, and your signature, all the information needed to forge checks or wire money out of your account. Finally, consider signing up for e-delivery of all bills and financial statements to avoid having sensitive information delivered to your mailbox, and pay bills electronically whenever possible.

If, despite your best efforts, you do become a victim of

23197 La Cadena Drive, Suite 103 | Laguna Hills, CA 92653
Direct: 800.545.4442 | Fax: 949.837.3604

identity theft, start by visiting identitytheft.gov. This government-run website enables you to report identity theft and provides you with a recovery plan based on your situation. Some of the steps in the recovery plan include notifying the defrauded creditors and each of the four credit bureaus, as well notifying your banks and credit unions. Your bank and credit union accounts will be closed once you notify them of the fraud, so you'll want to make sure that you immediately update automatic bill payments to the new account as well as notify your direct depositors so that you won't miss receiving any automatic deposits such as payroll or social security benefits. You also should file a report with your local police department and inform any other organization that holds your money, including investment and brokerage firms; and don't forget to tell your financial advisor as well about the fraud that's transpired.

2 **Get medical care or prescription drugs in your name.** If an imposter uses your identity to receive medical services, not only is the insurance company harmed, but fraudulent entries in your permanent medical record can impact your future eligibility for coverage and benefits. To avoid this, it's a good idea to carefully check your health insurance statements to make sure there haven't been any claims filed for procedures or office visits that weren't yours. And, if you have been a victim of any other form of identity theft, make sure you add your medical insurance providers to the list of people to contact when notifying them of your situation.

3 **File for social security benefits in your name (if you're eligible).** If you're age 62 or older and haven't yet filed to collect your social security benefits, beware — unclaimed social security benefits are a target for identity thieves. To make sure someone else doesn't start collecting your benefits before you do, create an online social security account at ssa.gov/myaccount and log in at least every six months to verify the accuracy of your personal information and your benefit status. If you find that something looks suspicious, call the Social Security Administration's fraud hotline at (800) 269-0271.

4 **File for unemployment benefits using your identity.** Recently, there has been an increase in fraudulent unemployment claims using stolen identities, particularly during the COVID-19 pandemic. Criminals filing for unemployment benefits using a stolen identity must, at the very least, have the victim's name, social security number, and date of birth. Be wary of telephone calls, text messages, letters, non-verified websites, or emails that require you to provide sensitive information, including birth dates and social security numbers. If you fall victim to this type of fraud, contact your employer and your state unemployment office to report the fraud and follow their instructions regarding resolution.

5 **File federal and state tax returns in your name.** Why would anyone want to file my tax returns, you may ask? To steal your refund, that's why! There are a few ways that you might discover this has happened. For example, you try to file your return electronically, but the IRS rejects it. The surest sign that you're the victim of tax-related identity theft is that the IRS prevents you from e-filing your return, which they will do if a return is already on file under your social security number. Or (if you prefer to file your taxes the old-fashioned way, by mail), you receive a letter from the IRS stating that a tax return with your social security number is already on file — another red flag. By the way, you should also know that the IRS will only contact you by mail — they will never call you or send you an email regarding fraudulent tax returns. Another sign that you're a victim of tax-related identity theft is that the IRS notifies you (again, by mail) that an online account was opened in your name. If you didn't open that online account yourself, then there's a good chance that someone is attempting to impersonate you with the IRS.

23197 La Cadena Drive, Suite 103 | Laguna Hills, CA 92653
Direct: 800.545.4442 | Fax: 949.837.3604

To protect your federal tax records, request an "Identity Protection PIN" (IP PIN) from the IRS. The IP PIN is a 6-digit number known only to you and the IRS, and is intended to prevent someone else from filing a federal tax return under your social security number. Check with your tax advisor to determine if the IP PIN program is a good option for you as there are some drawbacks. For example, you can't opt-out once you opt into the program; you must continue to use an IP PIN when you file your federal tax return. Another drawback is that your IP PIN changes annually. The IRS mails you a new IP PIN each January. If you lose or don't use the updated IP PIN, you will have difficulty filing your tax return. You can also check with your state taxing authority (for those of you who live in states with state income taxes) to see what methods they use to help prevent tax-related fraud.

6 **Claim the identity of a deceased person.** Yes, identity theft can happen even after someone passes away. This type of scam, called "ghosting," is more common than you might think. It can create additional anguish and inconvenience for loved ones tasked with straightening out the identity theft while also grieving their loss. A cybercriminal can use a deceased person's information to fraudulently open credit card accounts, apply for loans, get cell phones, and steal government benefits, among other things. There's often a significant lag between when a person dies and when government agencies or financial institutions are notified of the death and update their records. In the meantime, identity thieves can get personal information about deceased individuals by reading obituaries, fraudulently obtaining death certificates, or searching genealogy websites (many of which provide death records from the Social Security Death Index).

To avoid post-mortem identity theft, order several copies of the decedent's official death certificate (get more copies than you think you'll need) and provide one to all four credit bureaus, the IRS, and the decedent's financial institutions. You'll also want to notify the Social Security Administration (or ask the funeral home to do so) so that the SSA can lock the deceased's social security number, preventing changes to the address and the bank account where benefits are received. Other protection steps include watching for warning signs such as pre-approved credit cards or new bills in the deceased person's name, and avoiding disclosing too much personally identifiable information in the obituary, such as birth date, birthplace, full name, and relatives' names (including mother's maiden name).

As this discussion demonstrates, it's essential always to keep your private information private. When in doubt, err on the side of caution — if something seems fishy, it probably is. And if you're unsure, you can always reach out to a trusted advisor, family member, or your Towneley portfolio manager and ask, "Does this sound right to you?"

Over the next several weeks, we will continue this informative series with additional tips for how to protect your computer (PART 2) and how to identify common tricks and scams (PART 3). In the meantime, if it has to do with your personal information, the best rule of thumb is: **When in doubt, don't give it out!**

23197 La Cadena Drive, Suite 103 | Laguna Hills, CA 92653
Direct: 800.545.4442 | Fax: 949.837.3604