Privacy In A Digital World
DISCLAIMER OF LIABILITY AND WARRANTY

This publication describes the author’s opinions regarding the subject matter herein. The author and publisher are not rendering advice or services pertaining to specific individuals or situations. For specific advice, or if expert assistance is required, the services of a qualified professional should be obtained.

The author and publisher assume no responsibility whatsoever for the use of the information in this publication or for decisions made or actions taken based, in whole or in part, on the information in this publication. The author and publisher make no warranties, express or implied, regarding the information. Without limiting the foregoing, the author and publisher specifically disclaim and will not be responsible for any liability, loss, or risk incurred directly, indirectly or incidentally as a consequence of the use or misuse of any advice or information presented herein. Use this publication and information with good judgment and do the best you can in your particular situation.

You agree to indemnify and hold the author and publisher, and their respective officers, directors, agents, employees, contractors and suppliers, harmless from any claim or demand, including reasonable attorneys’ fees, related to your use or misuse of this publication or the information contained therein. You further agree that you will cooperate fully in the defense of any such claims.

Notice: As the owner of this electronic document you are permitted to store it and print it for your own personal use only. Otherwise, no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise without the prior written permission of the copyright owner and publisher. It is illegal to make a copy of all or part of this publication for someone else, even if you do not charge for the copy. If you have received this book from anywhere other than CardSafeGuard.com, including eBay, please report it to support@familysurvivalsystems.com immediately.

COPYRIGHT

Those who have received or purchased the guide are neither authorized nor permitted to transmit copies of this guide to anyone without written permission. Giving away copies to people who haven’t paid for them is illegal under international copyright laws and will submit you to possible legal action. Therefore, the utilization of this file is limited to personal use only.

TERMS AND DISCLAIMER

By using, viewing, and interacting with this guide or the CardSafeGuard.com and FamilySurvivalSociety.com websites, you agree to all terms of engagement, thus assuming complete responsibility for your own actions.

The authors and publishers will not be held liable or claim accountability for any loss or injuries. Use, view, and interact with these resources at your own risk.

All products from CardSafeGuard.com and FamilySurvivalSociety.com and their related companies are strictly for informational purposes only. While all attempts have been made to verify the accuracy of information provided on our website and within the publications, neither the authors nor the publishers are responsible for assuming liability for possible inaccuracies.
PRIVACY IN A DIGITAL WORLD

Once upon a time, identity thieves had to do things the old fashioned way. Combing cemeteries in search of deceased children, these unscrupulous people would log their names, then elaborately fool the Social Security Administration into releasing the social security number of the dead child. In some cases, identity thieves would even request a social security number from the SSA for a dead infant who was never even issued one. Then, these nefarious crooks would open bank accounts and obtain loans in the name of the dead child, and basically extract as much cash as possible out of benefits systems and banks until the source of income dried up. As recently as the 1980s, schemes like these were rarely found out because of the lack of computerization and communication. A prospective identity thief could ride the social security numbers of the deceased basically forever.

Nowadays, identity theft is much easier and much more rampant. The same tool that gives us incredible reach and function to deal globally is also the instrument of our demise – the internet. Using the internet, identity thieves can now obtain
far more information about you than they ever could by writing the SSA back in the day. They can obtain so much information in fact, that not only can they pretend to be you – they can actually be you. Identity thieves have managed to accomplish some pretty outrageous crimes as of late. Here is just a small sampling of what they can do:

• Project a false online presence, thus pretending to be you.
• Obtain credit cards and payday loans in your name with amazing rapidity
• Steal your credit card numbers in any manner of online sites
• Steal your credit card numbers from physical locations such as restaurants and stores
• Steal the details of your driver’s license by ‘reading’ the RFID signal your smart license broadcasts wherever you go

We’ll look at each of these items independently, but before we do, consider a few things. What is your identity, especially your digital identity? For example, what does your bank consider your identity to be in order to login to your account? It’s a shockingly low threshold – your identity can consist of as few things as your account number, your email address,
and your mother’s maiden name. These three pieces of information are all that is required in order to be you, as far as your bank is concerned.

IDENTITY THEFT – AN EXAMPLE

If you think an identity thief is some random lazy hacker in another country who only uses online means to steal your identity, you might only be partially right. Consider that sophisticated identity thieves are groups of highly experienced professionals who use all sorts of methods to steal your information and obtain credit in your name, steal your money, or impersonate you. What makes you the potential target of an identity thief? Just being alive, really. Identity thieves seldom target the rich or famous; these people have far too many resources at their disposal to combat such a theft and are usually aware of security breaches immediately.

You, Joe or Jane Sixpack, are far more likely to be the victim of identity theft. If you hold a job, have decent credit, and have a couple thousand dollars in the bank, you are a prime target. Identity thieves operate on an economy
of scale, pilfering small amounts from many people. Here’s an example.

You are being actively tracked by a group of identity thieves. The way they found you was simple — they cased your neighborhood by driving around in their car. They liked your suburban home; it was located in a decent but not high end neighborhood. You had a new car in the driveway; again, a midrange model that you probably had financed, meaning you are capable of obtaining credit.

The operation started quite innocuously; identity thieves paid a flyer delivery guy a hundred bucks to bring back the contents of your mailbox. While you were at work, this flyer delivery guy delivered a couple thousand flyers. Except when he reached your mailbox, he grabbed everything there was.

He reported back to the identity thieves, who he would never see again, and gave them your mail. Within was a cable bill, a water bill, and the jackpot — your bank statement. Armed with your name, address, and your bank statement, identity thieves quickly went to work. Although your account number was blocked out on your statement, the thieves were able to see that you had a handsome balance and also got a picture of where you spend your money.

Transitioning from the physical world of reading your mail, identity thieves then tracked down your online presence. A few simple keystrokes gave them your Facebook and Instagram pages, where you had carefully documented almost every facet of your
life in pictures. It wasn’t hard to track down your mom, who also had a Facebook, and learn her last name. This took less than ten minutes. Deciding that you were a worthy candidate for a theft, the identity thieves moved onto the next phase in their operation.

They parked outside your house in a nondescript vehicle, looking occupied or talking on the phone. What you didn’t know when you got out of your car was that you were being tracked with an RFID reader, which captured all of the data off your driver’s license. In a few short days, identity thieves knew where you lived, banked, shopped, and also knew critical pieces of information like your mother’s maiden name, driver’s license number, hair and eye color, and all sorts of biographical data about you.

Changing your bank account login would be elementary at this point. While most banks would send you a text stating that your login information has changed, most of the time identity thieves work at odd hours, when you are asleep or busy at work, and other times when such text might not be answered instantly. All they need is 15 short minutes, and they could take everything you have. It doesn’t take long! This is but one example. There are many others, and a myriad ways you could be ripped off.

HOW TO COMBAT IDENTITY THEFT AND ENSURE DIGITAL PRIVACY

The previous example is utterly horrifying to anyone who works for a living and stands much to lose from theft – basically, all
of us. There are some critical steps you can take to ensure that this doesn’t happen to you, however:

• **Protect your RFID smart cards with a blocking device.** If it has a microchip in it—passport, driver license, smart credit card or any other form of ID—it can be remotely read with widely available RFID readers. Blocking the signal these cards emit is simple—wrap them in tinfoil (this works, but not the most ideal solution), or purchase a dedicated RFID blocking product, such as the Card SafeGuard. These blockers will prevent unwanted intrusions into your digital privacy.

• **Watch your mail closely.**
In this day and age, most people discount snail mail as old fashioned and not worth protecting. Consider, however, that identity thieves routinely harvest your mail in order to learn more about you. They harvest your incoming mail to view your bills and statements; they also harvest your outgoing mail for checks, which contain your full name, address, routing number, and account number! There are two simple ways to defeat these methods: First, get rid of your mailbox, and cut a mail slot into your
home. This way, your mail gets delivered inside your home and does not sit in a box outside. Second, never send outgoing mail (especially checks) from your home. Drive to the post office and put them in the outgoing box directly. Some people prefer paperless statements, and this is a mixed bag. While the paperless bills don’t physically arrive at your house, they are easy to hack from your email account.

- **Never use accurate information when setting up online profiles.** Most banking and e-commerce sites will usually ask ‘secret question’ style data of you. In case you forget your password, you will often be asked things like your mother’s maiden name, name of your first pet, name of your high school, make of your first car, etc. *Never answer these questions truthfully!* The reason is simple – most of this data can be found out through social media. You might post a high school reunion picture which will reveal the name of your school. You might be linked with your mom in social media, and her information would be elementary to discover. Ditto for all the other data. Banks and e-commerce sites do not investigate or verify this information – so lie! Just make sure you can recall the answers. A neat trick to do so is to use the
last name of your best friend’s mother. It’s easy to remember and almost impossible for an identity thief to discover. If you already have this information entered in at various sites, change it now!

- **Limit your social media presence.** This is a big one. Most of us love social media; the mundane is suddenly fodder for endless rounds of pictures, posts, tweets, and videos. We tell people when we’ve left the house. We tell them where we are going, and in some cases, use GPS to reveal our precise location. We photograph everything including the inside of our homes, our kids, our cars, and lots of other sensitive information. Keep in mind that this information resides on the Internet forever. Besides the social media providers themselves, which basically archive this information permanently, consider that government agencies mine this data as well. Lastly, identity thieves also back up vast quantities of data for future mining purposes.

- **If you must use social media, be vague.** If possible, don’t reveal your true name, and use an email address that isn’t linked to your identity. You would be surprised at how many people use email addresses that have their whole name in them (example: ben.p.johnson@gmail.com). Ridiculous! Also, look for back doors that identity thieves use to learn more about you. Unless you actively disable them, most cell phones include geo-tagging information in the metadata of the pictures you take. In English, this means that GPS coordinates of all your photos are embedded in the photo
itself! This information is easy for hackers to find. They love finding little gems like you taking a picture of things like your gun safe, and knowing exactly where it’s located. Even after you disable geo-tagging, never take pictures of sensitive items like guns, jewelry, precious metals, etc.

• **Monitor the social media presence of your family.** You might abstain from social media, but make sure that your spouse or children aren’t revealing much of the same information you are trying to hide from others. Never link a social media account with anyone in your family or extended family. Run your name through a search engine periodically to see what comes up. Of course, this works better if you have a unique name. The goal here is to keep track of what you look like from an online standpoint. Knowing this will help you detect changes.

• **Pull your credit periodically.** By law, everyone gets one free annual credit report from the three credit reporting agencies (CRAs). These three are Experian, Trans Union, and Equifax. Scan your credit report for loans and entries that
don’t belong to you and other suspicious items. Delete old or unused addresses if possible. It’s even wiser to just pony up and pay to view your credit report every six months. What’s $50 compared to the theft of your identity?

• **Scan your bank account transactions daily.** Yes, daily! Most everyone has online banking these days. There is no reason why you can’t log in and view the previous day’s transactions. These could reveal theft or even simple error. For example, restaurants are havens for identity thief shills who discretely notate your credit card number when you aren’t looking. They can get the full number, your name, and the three-digit code on the back of the card easily. If you scan your statements daily, you can easily spot the misuse of your card data, and let your bank know immediately. Fraud is never your liability issue, especially if discovered rapidly. Identity thieves are counting on your complacence!

• **Shop online at reputable sites only.** By rights, online retail giants like Amazon and eBay are inherently secure, with entire departments of fraud personnel designed to protect your online shopping experience and information. Stick to bigger retail sites as they tend to be more. If you do need to order from a relatively new or small online store, double check that their order
process is secure. A secure online order page will display and web address/URL that starts with “https” the “s” stand for secure. You will usually see a green bar in the address bar or a little padlock symbol in or near the address bar. When you see this you’ll know the order page and order process is secure and your information is being transmitted in a safe, encrypted format. Ordering products and services online is a highly secure process if you just follow these simple rules of thumb. If you’re still wondering if the website is secure just phone them up and speak to a human first. Phone orders can actually be a bit more risky because you don’t really know the person you’re telling your payment information to, so just be aware. Luckily most credit card companies offer liability and fraud protection, you just need to keep an eye on your account statements to check for purchases you don’t remember making.

CONCLUSION

Be smart, and be vigilant. Identity thieves prey upon the complacent, and exist in the spaces that you don’t check very often. Don’t let them win by letting your guard down, and lastly, don’t assume that identity theft is purely a digital thing or something that happens only on the Internet. It can happen to you and your best protection is vigilance!