Chapter 3
Security Concerns, Passwords, Identity Theft, and Common Sense

It will be no surprise to anyone when I say that there are a lot of dishonest people in the world. As hard as you have worked to accumulate whatever you own, there are other people who are working just as hard to take it away from you. As I have learned over the years, honest individuals are those most prone to being the victims of dishonest individuals, because honest people assume that everyone else is equally honest, and therefore entrust others with their private information, or at least make it relatively easy to make their private information discoverable to others who may misuse it.

The opportunities to make this information available to someone who may misuse it have increased dramatically over the years. I remember when I was a child, I received my social security card on which it very clearly stated, "Not for identification purposes." Yet, over time, your social security number has become the primary identifier that you are who you say you are. It made sense for income tax purposes to be required to provide it to companies that needed to report your income, expenses, investments, insurance, credit reports, and any transactions that might impact your income tax liability. But it was, and still is, used in almost every other aspect of your life, such as your educational history, military service record, and even your medical history.

The same was true with birthdates. The people and companies asking for your birthdate were once using it to help identify who you were. But little thought was given to protecting this information from thieves. Even now, to schedule an appointment with your doctor, the person setting the appointment will often ask your birthdate before asking your name.

Nobody really thought much about it. People and companies asked for your social security number and birthdate and we willingly provided both bits of information to them. Not much thought was given to what others might be able to do with this information if it fell into the wrong hands.

I remember that many years ago, I regularly stored all my old paperwork in my garage. I had kept copies of every tax return I had filed since I was 16 years old, copies of bank and investment statements, real estate transactions, and much more. My social security number and birth date were everywhere, printed on seemingly everything.

In the house, more current records were regularly kept in drawers and home files, available for any guests or home workers to sneak a peek, if they so desired.

In discussing this chapter with others, it appears that most people did the same thing. They never thought about someone going through their old stuff. They were quite casual about keeping these records stored in their garages or homes. There were a few of them who prided themselves on being good about not being "packrats," and were quite proud of throwing stuff away. But upon further questioning, they admitted that they regularly purged their homes of this information simply by throwing these old records away in their trash. They now knew that there are some dishonest people that go through others' trash in the hopes of getting this useful information from the unwary.

I would venture a guess that if you, the reader, look around your house, you will find a lot of paperwork that contains one or more of the most dangerous personal identifying numbers, with could potentially be used to steal your identity or your money and destroy your credit.

As discussed elsewhere in this book, I long ago, shredded all unnecessary documents, scanned, and securely stored any information that might be of importance to me in the future. As I mentioned in my chapter on "Getting

Organized," I believe that a good starting point is investing in a good-quality cross-cut shredder to help eliminate the threat of accidentally sharing all the personal information contained in this paperwork.

The digital age in which we currently live has made it easier for us to do our banking, pay our bills, buy what we need, and have access to our important records online. It has also made it easier for thieves to steal our personal and private information, even if we are careful about designating whom we entrust with this information.

We can pay bills or make purchases by credit card, or by direct payment from our bank accounts, and we can have the choice whether or not to have the company or financial institution store our payment information online. But while this information is secure now, will some criminal mastermind figure out a way to get past the companies' safeguards?

It seems that we read about a new, massive security breach almost daily. Several million of us (including me) were affected by a security breach at Home Depot, requiring the issuance of new charge cards to all affected customers. Target was also affected by a similar breach, and we continue to read about such breaches time and time again. Major insurance companies have been hacked of both health and personal information. Even U.S. Government records have been hacked, potentially revealing the employment histories and records of several million workers.

There are a lot of brilliant criminal minds in the world. As fast as technological security advancements are made to help protect us from them, the criminals are just as rapidly discovering ways to get around these security enhancements.

As I am writing this chapter, credit cards are having chips embedded in them, presumably to provide additional security against information theft. Whether this will provide the additional security desired, we will know within a few years.

Apple, the innovative technology giant, has launched a new payment system that simply requires one to tap their smartphone against the payment device. I understand Android devices are about to do the same thing. How the payment information is conveyed securely is beyond my understanding.

Since technology changes so rapidly, for me to provide you with a list of precautions you should take to protect yourself and your important information would be a useless exercise.

However, a healthy dose of **common sense** can go a long way to protecting yourself. Don't make it easy for the thieves to get your information.

Start by identifying the information that is most useful to criminals, that which would help them to steal your identity, and gain access to your money and credit. This information should only be shared with those whom you trust completely. In my office, our standard protocol is to never provide this information in emails, unless the email is encrypted.

The information you want to protect includes your:

1. Social Security Number
2. Birthdate
3. Driver's License Number
4. Account Numbers
5. PINs (Personal Identification Numbers); and
6. Passwords

The Federal Trade Commission (FTC) has an excellent consumer information website with a lot of useful information regarding protection of your identity, and certain safeguards you can take to be more secure. The website is located

at www.consumer.ftc.gov/topics/identity-theft. I don't have sufficient space here to list all the useful information contained on the website, so I encourage you to check it out on your own; it may save you significant inconvenience and financial loss in the future.

If you have already been the victim of identity theft, the FTC also maintains a secure website with useful tips on how to recover from identity theft: www.identitytheft.gov. These tips include instructions on what to do right away, such as:

1. Calling the company or companies where you know the fraud occurred, speaking to the fraud department and asking them to close or freeze the accounts, then changing logins, passwords, and PINS for your account

2. Placing a fraud alert and getting your credit report from one of the three credit bureaus, if not all three (if you notify one, they are supposed to notify the other two for you). The FTC websites includes links to all three of the credit agencies:

    a. www.Equifax.com/CreditReportAssistance or call them at 1-888-766-0008
    b. www.Experian.com/fraudalert or call them at 1-888-397-3742
    c. www.TransUnion.com/fraud or call them at 1-800-680-7289

3. Report the identity theft to the FTC and fill out an Identity Theft Affidavit at www.identitytheft.gov or call them at 1-877-438-4338; which you should immediately print and save your FTC Identity Theft Affidavit; and

4. Take the FTC Identity Theft Affidavit along with your driver's license (or other government-issued ID with photo), proof of your address (such as a utility bill, lease, or mortgage statement), and any other proof you have of the theft; have the police file a report; and get a copy of the police report. Create your Identity Theft Report by combining the police report and FTC Identity Theft Report.

Following the steps listed above will give you the following rights. More detailed information about these rights is provided on the FTC website. You have the right to:

1. Place a 90-day initial fraud alert on your credit report
2. Place a 7-year extended fraud alert on your credit report
3. Obtain free copies of your credit report
4. Require fraudulent information to be removed (or "blocked") from your credit report
5. Dispute fraudulent or inaccurate information on your credit report
6. Stop creditors and debt collectors from reporting fraudulent accounts
7. Obtain copies of documents related to the identity theft
8. Stop a debt collector from contacting you

IMPORTANT: Immediate action is essential as it helps to limit your losses. For example, under most state laws, you're not responsible for any debt incurred on fraudulent new accounts opened in your name.

As for unauthorized credit card usage, under federal law, your liability is limited to $50.00. If you report the loss to the credit card company before it is used, you aren't responsible for any unauthorized charges to your account.

Your ATM or debit card can result in much higher liability to you if you don't promptly report the loss or theft of your card.

1. If you report the loss before any unauthorized charges are made, you are not liable for any losses

2. If you report the loss within two business days after learning about the loss or theft, your loss is limited to $50.00
3. Two business days after you learn of the loss or theft, but less than 60 days after your statement is sent to you, your loss is limited to $500.00; but
4. If you don't report it for more than 60 calendar days after your statement is sent to you, your loss is **potentially unlimited!**

Once you have taken the above steps to establish your Identity Theft Report, you should be sure to close any new accounts opened in your name, remove bogus charges from any of your accounts, correct your credit report, and continue monitoring your credit report periodically to watch for any additional fraudulent charges or accounts that may appear.

It may also be advisable to consider placing either a credit freeze on your account or adding an extended fraud alert on your credit. You can accomplish this by contacting all three of the credit bureaus, but unlike the creation of your Identity Theft Report, in which you need only contact one of the three credit reporting companies, the onus is on you to contact all three of them yourself.

More on Common Sense

Emails & Social Media: Think carefully about what you are saying in emails as well as what you are posting on the Internet. The 16-year-old daughter of a friend of mine was so proud when she got her driver's license, she took a picture of it and posted it on Facebook! This meant that her legal name, full address, driver's license number, and birthdate were now available to any thief and child molester who could see it.

Passwords: Who can remember them all? A common (but potentially dangerous) solution is to use the same password on all one's accounts and websites. I have well over 100 online accounts and websites I need to access, each with its own password. Some of the sites require that passwords be at least eight characters in length, and some must include a combination of uppercase and lowercase letters, numbers, and special symbols. In addition, some of my work-related websites require my password to be changed every 90 days.

One solution is to have a written list, as in the attached "Everything" file. But don't leave it in a place where it can be found by someone you don't want having access to it. You may want to leave it in your safe deposit box at the banks for your representative to be able to get in the event of your incapacity or death. But be sure to update it regularly.

Another solution is to have an encrypted file on your computer that requires a password to access. This will enable you to be able to keep it updated as needed, and be available to you to use when you can't remember your own passwords.

Possibly the best solution is to use a **password manager** that stores your passwords in an encrypted file, which is then secured by a master password. Some additionally require that a key file must be present for the password database to be unlocked, often on an external USB stick. There are far too many such services available for me to list them, and rapidly changing security protocol will render any recommendations I provide here obsolete by the time this book is published.

Remember that someone else handling your affairs will need access to all your accounts and websites to enable them to handle your affairs, so either provide them with a copy of them (and be sure they will be as careful with their protection as you would be), or let them know where the list is located, such as in your safe deposit box, and how to access it and the information contained in it, if it is digital.

Only you can determine what is best for your security comfort level, so be sure to do your own research on what password management system will work best for you.

Storage of old records

Your information may be stored in numerous locations. In my chapter on "Getting Organized," I discussed all the physical paperwork and records that are stored in boxes or file drawers in your garage, storage shed, basement, or attic. Also remember to look in your home office, kitchen, bedroom closet, shelf, or dresser drawer. And, of course, you may also store a lot of your personal information at your workplace. Finally, don't forget about your safe or lockbox.

Digital media is also quite prevalent. Over the years, data has been stored on old 5-1/4 inch or 3-1/2 inch floppy drives and zip drives. More recent storage includes the use of CD-ROM and DVDs, USB drives, and external hard drives.

Most recent additions include cloud-based storage, some of which require a subscription from you, others that do not.

And don't forget your old computers, even if they no longer work. The hard drive still contains a lot of information that should be destroyed before throwing away the old computer. This applies to your old smartphones, too.

There are programs available that help to totally destroy the data on a hard disk. I'm not sufficiently computer savvy to know which ones to use, let alone recommend. So, personally, I'm still a fan of using an old-fashioned hammer physically smashing hard drives and storage devices into little pieces, and scattering them between several different disposal locations.

Here are some more common-sense ideas for you to consider:

1. Scan and Shred

As described in greater detail in the chapter on "Getting Organized," one of the best things you can do is to eliminate as much of the paperwork you have accumulated over the years, particularly the paperwork that contains your personal information (see paragraph 2 below). Consider investing in a high speed, high-quality scanner with a multi-page feed slot, and save your piles of documents in digital format.

At the time of writing this book, I use the Fujitsu Scansnap ix500, which holds 50 pages in the feed slot, and can scan 25 double-sided color pages per minute. While at $429.95, it is pricey, but it is a true workhorse, and will pay for itself in saved time, particularly compared to one-page-at-a-time scanners. If you need to justify the expense, think of it this way: If you earn $15.00 per hour, it will pay for itself in 30 hours (i.e., one hour of scanning per day for a month).

Once you have scanned, named, and saved the document, unless it is an important document that must be saved in its paper form, you can now shred it. There are many types of shredders available that will do the job, but once again, don't buy a cheap one. Invest over $100.00 to get a cross-cut shredder that won't jam if you try to shred over 10 pages of paper at a time.

By scanning and shredding, you now have fewer documents you need to worry about getting into the hands of thieves.

2. Keep your personal information in a secure place

What is your "personal information?" Your social security number, birth date, driver's license number, passport number, account numbers, etc. All of these items can be used to steal your identity.

Whether at home or at work, there are workers or cleaning services, not to mention nosy relatives and friends, who may just take a "peek" at the papers on your desk. Don't leave your credit cards, debit cards, driver's license, passport, or any paperwork containing any of this information anywhere other than in a locked or secure place.

And for those individuals who leave credit cards in their automobile "for convenience" purposes, you are making it convenient for the thieves, too.

3. Storage devices and storage in the cloud

Just because you have eliminated the paper, you're not done. You still need to secure the digitized documents wherever you store them. Whether you store them on your computer, on an external storage device, in the cloud, or elsewhere, the devices and/or the documents containing your personal information should be encrypted and/or password protected.

4. Phone calls and emails

Unless you absolutely know and trust the person who is calling you or sending you texts or emails, do not give anyone your personal information. And don't click on suspicious links, even if you know who sent them to you. For example, you get an email from a friend, but there is no message, only a link to click. It is worth taking the time to call the person to confirm they sent it.

5. Review your credit report annually

Take advantage of the ability to review your credit report from each of the three major credit reporting agencies for any irregularities. You can obtain a report for free once a year. If anything looks suspicious, it is worth a follow-up call to the creditor named. Similarly, if you are denied credit, find out the reason and make sure it is legitimate.

6. Review your bank statements and credit card statements

Take a moment to review your bank statements and credit card bills carefully for wrong or fraudulent charges. If you don't recognize a charge, investigate it. Consider adding a monitoring feature on your bank accounts. For example, I receive an email from my bank anytime a payment goes out of my account exceeding $100.00. I caught three back-to-back eBay.com purchases allegedly made by me, which were paid through PayPal via my bank account. I succeeded in intercepting the phony charges within minutes. Of course, I changed passwords, and reported the security breach to eBay and PayPal, both of whom were very helpful in resolving the issue.

7. Secure sites

It took me a long while to become comfortable paying bills and purchasing goods online. I learned to make a point of looking for a website address beginning with **https** in the website address URL bar to make sure the site I was using was secure. This may be too technical, but "**HTTPS"** stands for **Hypertext Transfer Protocol *Secure***, and instead of acting as its own application layer protocol, it uses separate protocols called SSL (Secure Sockets Layer) and TLS (Transport Layer Security). The SSL encrypts the information that is being sent, which means that the true meaning of the data (credit card numbers, personal information, etc.) is very difficult to be cracked by anyone trying to see the information. Nowadays, most web browsers support HTTPS for more secure Internet browsing. Browsers such as Internet Explorer, Google Chrome, and Firefox will display a padlock icon to identify a secure HTTPS connection to a website.

8. Compile a list of your accounts

Maintain a record of all your credit card and debit card numbers, so you have a cross reference if an unexpected bill appears with a different account number. Call the credit card company **immediately**. Don't wait!

9. Use firewalls, anti-spyware, and anti-virus software to protect your home and work computers

Be sure to keep them up to date!

10. A final comment about common sense

As I learned in law school, “If it sounds too good to be true, it probably is!” This applies to your digital security, too. Trust your instincts. If something doesn’t seem quite right, or if you find yourself pausing before clicking on a link or giving out personal information in an email or over the telephone, don’t do it until you have verified you are giving it to a legitimate source.

I anticipate a time will come when, for security purposes, we will all have microchips imbedded somewhere in our body. But I am also aware that, as quickly as the security firms can create new, safer, innovative methods to keep our data secure, there are brilliant thieves developing new, creative methods to steal our information, our money, and our identities. As hard as we all work to earn our money, there are thieves working just as hard to try to take it away from us. Be careful and use common sense.