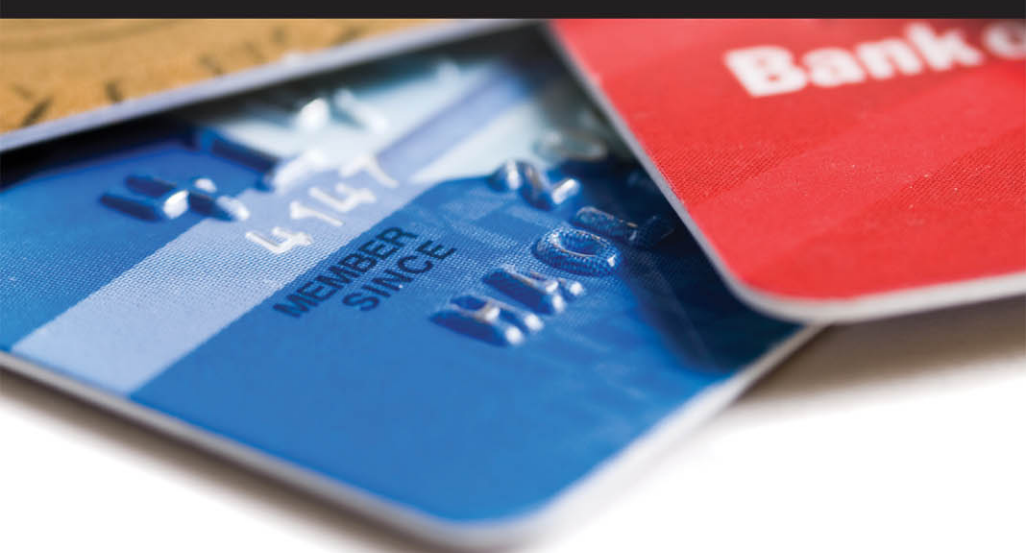
More Than 200 Million People at Risk Right Now...

IDENTITY THEFT ALERT

10 RULES YOU MUST FOLLOW TO PROTECT YOURSELF FROM AMERICA'S #1 CRIME



STEVE WEISMAN

Praise for *Identity Theft Alert*

"Identity theft is everyone's opponent, but just like in basketball, the harder you prepare, the better your chances of winning. Steve Weisman shows you what you need to do in order to protect you and your family from identity theft."

John Calipari, head basketball coach, University of Kentucky

"There are people out there determined to wreck your life by stealing your identity. Nobody better prepares you to fight back than Steve Weisman. His new book, *Identity Theft Alert*, is why Steve's the guy I always turn to on this topic, on my 500 radio stations coast to coast. Steve should be the defensive coordinator of your identity, as well."

Jim Bohannon, nationally syndicated talk host, Dial Global Radio Networks

"Scammers, hackers, and thieves of all stripes should consider themselves warned. Steve Weisman is on to you and has armed the American people with knowledge, the most powerful tool of all. Comprehensive in scope, urgent in tone, *Identity Theft Alert* is a must-read for anyone concerned about identity theft...and that should be all of us."

Stan Rosenberg, Massachusetts State senator

"Identity theft has become the number one property crime in America today, and it can disrupt your life tremendously. What you don't know about identity theft can hurt you, but fortunately in this brilliant book Steve Weisman, a leading expert on identity theft, provides you with the tools you need to protect your identity."

Thom Hartmann, nationally and internationally syndicated radio and television talk show host; author of four *New York Times* bestsellers

"Steve's strength is staying ahead of the latest threats. Through his many guest appearances, he has provided my viewers with the information they need to prevent identify theft before it occurs. His new book puts his valuable knowledge all in one place and is a comprehensive plan for protecting yourself against identify theft."

Mike Nikitas, news and business anchor, NECN (New England Cable News)

"Steve Weisman's latest book, *Identity Theft Alert*, is essential reading for anybody who has a credit card, a credit history, a bank account; owns a phone; uses the Internet; or earns money for a living. Steve offers a sobering look at how scam artists operate. More importantly, the book offers practical advice on how best to protect yourself from these dangerous threats."

Mike Baxendale, co-host of the *Bax & O'Brien Show*, WAQY, Springfield, Massachusetts

"It seems like every day, there's a new story about identity theft grabbing headlines. As a frequent guest of our morning show, I'm always impressed by how quickly Steve learns about these scams and their intricacies. He consistently delivers practical, easy-to-digest advice about how to prevent falling victim. Whether we're shopping with a credit card or surfing the Web, we expose so much personal information on a daily basis, making *Identity Theft Alert* a must-read."

Emily Volz, anchor, WGGB-TV, Springfield, Massachusetts

"Steve Weisman's knowledge of scammers and thieves in unmatchable. As a regular on our morning newscast, he has brought our viewers critical and timely information that has been invaluable in protecting them. His latest book is a must-read in this increasingly vulnerable world!"

Tom Lewis, anchor, WGGB-TV, Springfield, Massachusetts

"Identity theft is one of the largest growing areas of crime, and in today's digital world it gets more difficult to know if we are safe. Thank goodness we have Steven Weisman to help us in this easy and fun-to-read guide."

Alan Colmes, *Fox News*

Identity Theft Alert

10 Rules You Must Follow to Protect Yourself from America's #1 Crime

Steve Weisman

Associate Publisher: Amy Neidlinger
Operations Specialist: Jodi Kemper
Cover Designer: Chuti Prasertsith
Managing Editor: Kristy Hart
Senior Project Editor: Betsy Gratner
Copy Editor: Cheri Clark
Proofreader: Debbie Williams
Senior Indexer: Cheryl Lenser
Senior Compositor: Gloria Schurick
Manufacturing Buyer: Dan Uhrig

Publishing as FT Press
Upper Saddle River, New Jersey 07458

Printed in the United States of America

Second Printing: November 2014

ISBN-10: 0-13-390252-8
ISBN-13: 978-0-13-390252-5

Pearson Education LTD.
Pearson Education Australia PTY, Limited
Pearson Education Singapore, Pte. Ltd.
Pearson Education Asia, Ltd.
Pearson Education Canada, Ltd.
Pearson Educación de Mexico, S.A. de C.V.
Pearson Education—Japan
Pearson Education Malaysia, Pte. Ltd.

Library of Congress Control Number: 2014939199

To Carole for yesterday, today,
and all our tomorrows

This page intentionally left blank

Contents

Acknowledgments

Many people have supported and encouraged my efforts in creating this book, and although I cannot name every one, I do want to mention a few.

Marc Padellaro, who teaches me more about everything every day and for whose friendship I am eternally grateful. He is a mensch above menschen.

Roger Weisman, who inspires me with his breadth of knowledge and insight.

Laurie Swett, my first and longest supporter, who really is as nice as people think she is.

Michael Harrison, my great friend and mentor.

Ron Nathan, a friend I can always count on.

Mark Peterman, Janice Peterman, and Laurie Priest of the peaceable kingdom, who help keep me centered.

Joe Newpol, Iris Berdrow, and Aaron Nurick, my colleagues at Bentley University who educate me as they do their students.

Saul Chadis, Peter Ettenberg, Marty Kenney, Bruce Newman, and Peter Seronick, whose friendship and support has stood the test of time—a long time.

Jennifer Sayles, my physical therapist, whose efforts enabled me to be able to type again. To quote John Mellencamp, "She hurts so good."

About the Author

Steve Weisman hosts the radio show *A Touch of Grey*, syndicated to 50+ stations nationwide, including AM 970 (NY) and KRLA (LA). A senior lecturer at Bentley University, he is a lawyer and is admitted to practice before the U.S. Supreme Court. He is also the legal editor of *Talkers Magazine* and a commentator on scams and identity theft for television station ABC 40 in Springfield, Massachusetts. He writes for publications ranging from the *Boston Globe* to *Playboy* and earned an ABA Certificate of Merit for excellence in legal journalism. His books include *The Truth About Avoiding Scams*, featured on Dr. Phil and CNN. Weisman holds a J.D. degree from Boston College Law School. He also operates the website www.scamicide.com, which provides the latest information on scams and identity theft.

Introduction

Identity theft is one of the most pervasive and insidious crimes of today, a crime that can tremendously disrupt your life—or even put you in jail for crimes you never committed.

This book explains the horrific details of the many identity theft scams that are so prevalent today. Story after story takes you into the dark world of identity theft and the dire consequences that can result from this crime that affects more and more people throughout the world. This book shows you just how vulnerable you are, but it also shows you steps you can take to protect yourself, as best you can, from becoming a victim. It also tells you what to do if you become an identity theft victim.

Identity theft is the biggest and fastest-growing crime in the world and with good reason. It is easy to perpetrate and easy to get away with.

No one is immune from identity theft—children, the elderly, and even the dead can have their identities stolen.

Through modern technology, an identity thief half way round the world can steal your identity from your computer, your laptop, your iPad, or your smartphone.

I can teach you how to recognize the risks of identity theft and how to avoid them.

What you don't know *can* hurt you. I will tell you how to spot dangers in places you might never have considered, such as your television, your cellphone, or even a copy machine.

In this age of information sharing, everyone is particularly vulnerable to identity theft because even if you are doing everything right, the many companies and institutions with which you do business and operate in your everyday life might not be protecting you as much as they can. I can show you how to minimize those risks.

This book might scare the hell out of you, and rightfully so. It explains just how vulnerable we all are in the world of identity theft. But it also

tells you specifically what you can do to reduce your chances of becoming a victim and precisely what to do if you do become a victim of identity theft.

Many years ago, I worked as a professor in a college program in the state prison system in Massachusetts. One of my students was serving two consecutive life sentences, which meant that after he died, he would start his second sentence. When he told me about this, I told him how I had always wondered how that worked. He said that he had, too; when he was sentenced, he yelled at the judge, "How do you expect me to do two consecutive life sentences?" to which the judge responded, "Just do the best you can."

There are no guarantees in life and there certainly is no guarantee that you will not become a victim of identity theft; but by reading this book, you will learn how to do the best you can, and you can certainly narrow your chances of becoming a victim.

Bonus Online Content

You can access bonus content for this book at www.ftpress.com/identitytheft. There you'll find form letters and more information about the Gramm-Leach-Bliley Act, credit reports, identity theft insurance, identity theft and the elderly, and more.

This page intentionally left blank

1

Identity Theft

Identity theft can result in your being hounded by debt collectors for debts you did not incur; becoming unable to access your own credit cards, bank accounts, or brokerage accounts; having your assets stolen; being arrested for crimes committed by people who have stolen your identity; or even receiving improper medical care because your medical identity has been stolen and your medical records have been corrupted. In addition, identity theft can ruin your credit rating, which can affect your chances to get a loan, get a job, get insurance, or rent a home.

Identity theft is the number-one consumer fraud in America, according to the Federal Trade Commission. According to a study by Javelin Strategy & Research, there were 12.6 million victims (which actually might be as many as 16.6 million victims) in 2013. According to the Justice Department's Bureau of Justice Statistics, the cost of identity theft to its victims in 2013 was $24.7 billion, which is $10 billion more than the cost of all other property crimes combined, and the crime is getting worse. As the global village becomes smaller and smaller due to the Internet, the conditions for international criminals committing identity theft from a world away have become greater. Unfortunately, as technology has continued to advance, legislative efforts to combat identity theft have not kept pace.

Terrorism and Identity Theft

Although the connection between terrorism and identity theft might not be immediately apparent, it is very real and threatening.

In his testimony of September 9, 2003, before the Senate Committee on Finance regarding the homeland security and terrorism threat from document fraud, identity theft, and Social Security number misuses, FBI acting Assistant Director of the Counterterrorism Division John S. Pitole said, "Advances in computer hardware and software, along with the growth of the Internet, have significantly increased the role that identity theft plays in crime. For example, the skill and

time needed to produce high-quality counterfeit documents has been reduced to the point that nearly anyone can be an expert. Criminals and terrorists are now using the same multimedia software used by professional graphic artists. Today's software allows novices to easily manipulate images and fonts, allowing them to produce high-quality counterfeit documents. The tremendous growth of the Internet, the accessibility it provides to such an immense audience, coupled with the anonymity it allows, result in otherwise traditional fraud schemes becoming magnified when the Internet is utilized as part of the scheme. This is particularly true with identity theft–related crimes. Computer intrusions into the databases of credit card companies, financial institutions, online businesses, etc., to obtain credit card or other identification information for individuals have launched countless identity theft–related crimes.

"The methods used to finance terrorism range from highly sophisticated to the most basic. There is virtually no financing method that has not at some level been exploited by these groups. Identity theft is a key catalyst fueling many of these methods. For example, an Al Qaeda terrorist cell in Spain used stolen credit cards in fictitious sales scams and for numerous other purchases for the cell. They kept purchases below amounts where identification would be presented. They also used stolen telephone and credit cards for communications back to Pakistan, Afghanistan, Lebanon, etc. Extensive use of false passports and travel documents were used to open bank accounts where money for the mujahidin movement was sent to and from countries such as Pakistan, Afghanistan, etc."

When Al Qaeda leader Khalid Sheikh Mohammed, who was described in the 9/11 Commission Report as the "principal architect of the 9/11 attacks" on the United States, was captured in 2003, his laptop contained more than a thousand stolen credit card numbers.

According to a report on Identity Theft & Terrorism prepared by the Democratic Staff of the Homeland Security Committee in 2005, "Terrorists also steal identity information to gain access to credit or cash that can be used to finance their operations."

Who Are Identity Thieves?

Identity theft is an equal-opportunity crime. Identity theft is done by organized crime both in the United States and in foreign countries around the world, particularly Eastern Europe. Much of the rash of recent hackings of companies and government agencies in order to steal personal information to be used for identity theft purposes can be traced back to Russia. A 17-year-old Russian hacker, Sergey Taraspov, is thought to have written the computer program used to attack Target late in 2013. Taraspov is alleged to have sold the program on the black market for $2,000.

Although the name of Bulgarian Aleksi Kolarov is probably not familiar to you, it probably should be. In 2014 he was convicted of identity theft in federal court in New Jersey. For years, Kolarov was one of the leaders and operators of the website Shadowcrew.com, a black market website where stolen credit cards, debit cards, and bank account information were sold to the approximately 4,000 members of the criminal website. It has been estimated that Shadowcrew was responsible for the theft of 1.5 million credit cards, debit cards, and bank account numbers, resulting in fraud losses totaling millions of dollars to the banks issuing the cards.

According to the FBI, a Russian organized crime gang responsible for the data breach at Neiman Marcus in 2013 was also responsible for the theft of more than 160 million credit cards from numerous other retailers over the previous seven years.

Identity theft, however, is not solely the province of organized crime. It is done by small-time hoodlums, street gangs, your fellow workers, and even members of your own family.

What Do Identity Thieves Do?

Identity thieves take your personal information and use it to harm you in various ways, including these:

- Gaining access to your credit card accounts, bank accounts, or brokerage accounts
- Opening new credit card accounts in your name
- Opening new bank accounts in your name
- Buying cars and taking out car loans in your name
- Using your name and credit to pay for utilities, such as fuel oil or cable television
- Buying smartphones and phone plans in your name
- Using your medical insurance to obtain medical services, thereby corrupting your medical records
- Renting a home
- Using your name when committing crimes, for which you can be arrested

Although you might not be responsible for fraudulent charges made by an identity thief using your name, the damage to your credit as reflected in your credit report can affect your future employment, insurance applications, and loan applications, as well as future credit arrangements you might want to establish.

College Students and Identity Theft

College students are five times more likely to become victims of identity theft than the rest of the population, and they usually take longer to find out that they have been victimized. Living in close quarters and a lack of proper precautions are circumstances that make college students easy pickings for identity thieves.

TIP

Here is a list of things that college students should do to protect their identity:

- Lock computers, smartphones, and tablets when they are not in use
- Use a strong password and use different passwords for each device
- Use encryption software on all electronic devices
- Don't use Wi-Fi for financial transactions; it is too easy to infiltrate
- Because college mailboxes are not very secure, have sensitive mail sent home or sent to the student electronically
- Don't trust messages with links from "friends" that appear on the student's Facebook page
- Don't put too much personal information on Facebook pages; it can lead to identity theft
- Shred papers containing personal information before disposing of them
- Check bank statements and credit card statements carefully each month to look for signs of identity theft
- Get a free credit report from each of the three credit-reporting agencies annually

Malware and Macs

For many years, users of Apple computers have felt safe knowing that, by and large, most computer scams targeted users of PCs rather than Macs. However, with the increasing popularity of Apple computers and portable devices, more and more scammers and identity thieves have begun to tailor their illegal activities to Mac users. In the past, identity thieves often targeted their malware attacks against PCs because there were more PC users than Mac users. But now identity thieves and hackers focus much of their attention on Macs.

If you are a Mac user, you should have your computer checked for the presence of malware. Every computer user should have up-to-date security software that automatically updates and protects it from the latest malware and viruses.

Dumpster Diving

Dumpster diving is the name for the practice of going through trash for "goodies" such as credit card applications and other items considered to be junk by the person throwing out the material. In the hands of an identity thief, some of this trash can be transformed into gold in ways an early alchemist could never have imagined. Go to any post office and inevitably you will find in their trash containers much of this information that owners of post office boxes toss out when they go through their mail before they leave the post office. Too often people do not even bother to tear up the items. In the case of preapproved credit card offers, all the identity thief has to do is fill in the application, change the address, and send it back to the bank. In short order the thief will receive a credit card, and a careless individual will become the victim of identity theft as the identity thief begins to use the credit card and runs up debt in the victim's name.

You Are Only As Safe As the Places That Have Your Information

You will find that one of my recurring themes is that regardless of how careful you are about protecting your personal information from identity thieves, you are only as safe as the places that hold your personal information. These places include companies with which you do business, governmental agencies, and any club or association to which you belong. It is not unusual for rogue employees to steal the personal information of customers or members and either use it themselves for identity theft or sell the information to professional identity thieves. It is also important to note that small retail businesses have recently become a prime target for identity thieves because identity thieves have found that many of these businesses do not pay sufficient attention to maintaining the privacy and security of the personal data they hold.

So what can you do?

One thing you can do is try to limit as much as possible the personal information, particularly your Social Security number, that you provide to third parties. The Social Security number is a key element in identity theft. Armed with that number, an identity thief could find it a simple matter to steal your identity. Many establishments with which you do business routinely ask for your Social Security number even though they have no legitimate need for it. Recently, I was asked for my Social Security number when I went to my eye doctor. I responded by politely asking if it would be acceptable for me to provide my driver's license instead, and they were willing to accept that.

They Should Know Better

In recent years, large law firms have become a target of identity thieves because they have not instituted the proper data security measures necessary to protect the vast amounts of information they hold that, in the wrong hands, can lead to identity theft. As long ago as 2011, the FBI warned major law firms of the dangers of identity theft and corporate espionage, particularly law firms with foreign offices in China and Russia. However, not enough law firms have heeded these warnings, and many continue to put unencrypted information on thumb drives, e-mail unencrypted information to smartphones and iPads that are not secure, and use unsecured networks in countries such as China and Russia where hacking is rampant. Fortunately, many law firms are changing their practices under pressure from clients such as large banks who are threatening to withdraw their legal business unless proper security is initiated.

Hackers

Computer hacking of government and private business computers has resulted in the personal information of millions of people being compromised. Whereas at one time, the hacking of companies and businesses required considerable technological acumen, now cybercriminals need only go online to black market websites where they can purchase the necessary malware required to steal information from a targeted company or government agency. According to Trend Micro, a Japanese security software company, one particular type of hacking malware called BlackOS can be purchased on the black market for $3,800.

NO CURE FOR STUPID

According to comedian Ron White, "There is no cure for stupid." Far too often, owners of laptops or other portable electronic devices pave the way for identity thieves to gain access to personal information merely by stealing devices containing unencrypted personal information.

Identity Theft Risk in Old Gaming Consoles

Avid video game players are always excited about the release of the latest version of the popular consoles. Gamers who purchase the new gaming consoles generally sell their older gaming consoles on eBay or other sites after buying the newer version. To the surprise of many people, this can lead to identity theft. Video game consoles such as the Xbox and PlayStation are not just video game players, but also quite sophisticated computers that often have important personal information, including credit card information, stored on the computer's

hard drive. Identity thieves know this and buy the used gaming consoles to harvest the personal information from the consoles and make their former console owners victims of identity theft.

If you are selling or otherwise disposing of your older video game consoles, make sure that you remove all personal information from the hard drives before you sell or get rid of them. The simplest way to do this is to get an external hard drive reader that you can use to connect your console's hard drive to your computer. After it is connected to your computer, you can use a program such as "Eraser," which is free, to remove your personal information from your console's hard drive.

The Drug Connection

Steven Massey was convicted of conspiracy to commit computer fraud and mail theft for his operation of an identity theft ring in which he enlisted methamphetamine addicts to plunder mailboxes and a recycling center for preapproved credit card applications and other material that could be used for identity theft. Methamphetamine addicts are perfectly suited for the crime of identity theft. They often stay awake for days at a time and can patiently perform boring tasks such as going through mail and even piecing together torn credit card solicitations. Drug money for identity theft information is a growing problem throughout the country.

TIP

When you are disposing of any papers or documentation that has personal information that, in the wrong hands, could be used to make you a victim of identity theft, it is important to first shred the documents before you dispose of them. However, you should remember to use a crosscut shredder rather than one that makes only vertical cuts because some identity thieves actually take the time to reconstruct documents that have been only vertically shredded.

Phishing

The term "phishing" goes back to the early days of America Online (AOL) when it charged its customers an hourly rate. Young Internet users with an addiction to their computers, not very much cash, and a bit of larceny in their hearts sent e-mails or instant messages through which they purported to be AOL customer service agents. In these phony e-mails, under those false pretenses, they would ask for their unwary victims' passwords in order to stay

online on someone else's dime. After a while, this phony expedition, fishing for information, became known as "phishing."

Now, phishing is the name of the scam whereby you are lured to a phony website that appears to be legitimate, but when you click on links in these phony websites, download material from these websites, or provide information to these websites, you put yourself in danger of identity theft or of downloading dangerous keystroke-logging malware that can steal all the information on your computer including credit card numbers, your Social Security number, passwords, and various account information.

Federal Express Phishing Scam

Federal Express has often been the subject of phishing. Many of these phishing scams have come from the e-mail address of BillingOnline@fedex.com. These e-mails generally refer to a Federal Express invoice for which you are being billed. These are scam phishing e-mails, and if you enter personal information in order to dispute the bill, this information will be used to make you a victim of identity theft. You also might unwittingly download keystroke-logging malware that can steal the information from your computer and make you a victim of identity theft.

Federal Express does not send unsolicited e-mails requesting information regarding packages, invoices, account numbers, or personal information. If you receive such an e-mail, it is a scam. Do not open it and do not click on any links. If you have any questions as to the legitimacy of a Federal Express bill, contact them directly by phone or online at www.fedex.com.

Newegg Phishing Scam

Newegg.com is a legitimate company that sells computer and electronic products. Identity thieves have been sending phishing e-mails that look as though they have been sent by Newegg informing the recipient that his or her online sale has been completed and charged to his or her credit card. The notices look real, the logo looks accurate, and the bill doesn't have the grammatical mistakes found in many such scams. However, it is nothing more than a phishing scam. If you click on links within the e-mail in order to question the order, you will unwittingly download harmful malware onto your computer.

I actually received one of these scam phishing e-mails and took my own advice, which is whenever you have a question about the legitimacy of such an e-mail, call the company at a number that you know is accurate. So I called Newegg. Before I could even ask a question, a recording informed me that the invoice was a scam.

Former Good Advice

Smug consumers used to be able to identify a phishing expedition by merely looking at the Web browser's address window to determine whether the e-mail purporting to be from some company with which they generally dealt was legitimate. If the sender's e-mail address began with an unusual number configuration or had random letters, this indicated that it was phony. The e-mail addresses of legitimate companies are usually simple and direct. Unfortunately, this is not always the case. Now computer-savvy identity thieves are able to mimic the legitimate e-mail addresses of legitimate companies.

More Good Advice to Avoid Becoming a Victim of Phishing

Don't fall for the bait. It takes a few minutes longer, but if you are in any way inclined to respond to an e-mail that could be phishing to send you to a phony website do not click on the hyperlink in the e-mail that purports to send you directly to the company's website. Rather, type in what you know to be the proper website address for the company with which you are dealing.

As more people become aware of the dangers of phishing, identity thieves are adapting their tactics to use Internet search engines, such as Google or Bing, to lure people into clicking on links that people think will send them to a legitimate website, but that instead will download dangerous malware to their computers that can steal all the information on their computers and make them victims of identity theft. Identity thieves have been able to infiltrate search engines by adapting their phony websites that contain these dangerous links to be positioned on search engines to receive more traffic. People are less aware of this danger and are less skeptical of search-engine results than they are of e-mails with phony phishing links.

TIP

Many of the tainted websites are tied to celebrity news, such as videos of the latest Justin Bieber arrest or news of major world events that capture the public's interest. Identity thieves exploit the curiosity of the public with promises of tantalizing videos or stories. If you are searching for such information, you should limit your searches to websites that you know are legitimate. Because many of these search-engine phishing scams are based in Russia and China, you should be particularly wary of websites with links that end in .ru (Russia) or .cn (China). Both Google and Microsoft, which operates Bing, are acting to combat this type of scam, but it is a difficult task and you should not expect a solution soon.

The mysterious disappearance of Malaysian Airlines Flight 370 in 2014 captured the attention of people around the world, so it should come as no surprise that scammers and identity thieves promptly used this event as an opportunity to steal people's identity through malware-infected phony news reports, photos, and videos. In 2011 similar scams tied to the Japanese tsunami were common. Throughout the Internet and on social media, including Facebook and Twitter, following the disappearance of Malaysian Airlines Flight 370, links to phony stories, photos, and videos appeared with tantalizing headlines such as "Shocking video, Malaysian Airlines missing flight MH 370 found in Sea," "Malaysian Airlines missing flight MH 370 found in Sea—50 people alive saved," and "CNN UPDATE Breaking—Malaysian Airplane MH 370 Already Found. Shocking Video." Some phony links even promised videos of the plane in the Bermuda Triangle. Unfortunately, if you clicked on these links, all you succeeded in doing was unwittingly downloading keystroke-logging malware that could steal your personal information from your computer, laptop, tablet, or smartphone and use that information to make you a victim of identity theft.

The Dangers of Aquaman

Many people are fascinated by superheroes such as Superman, Green Lantern, and Batman. But you should always remember that whatever fascinates large numbers of the public also sparks the interest of identity thieves. These criminals set up phony websites and links on these websites that are traps for the unwary and can result in Internet surfers downloading keystroke-logging malware that can steal all the information from your computer and make you a victim of identity theft. Security software company McAfee released a list of the most dangerous superheroes of the Internet. Surprisingly, at the top of the list, with 18.60 percent of searches resulting in tainted websites, is DC superhero Aquaman, which is surprising because he doesn't even have a movie. Close behind Aquaman, at 18.22 percent, is Marvel Comics' Mr. Fantastic. The rest of the list in order is The Hulk, Wonder Woman, Daredevil, Iron Man, Superman, Thor, Green Lantern, Cyclops, Wolverine, Invisible Woman, Batman, Captain America, and last but not least your friendly neighborhood Spider Man, who, although having only 11.15 percent of tainted websites, still poses a significant risk to the unwary. Thus, Aquaman is even more dangerous than the most dangerous woman on the Internet, Emma Watson of Harry Potter fame. Internet searches of her will lead you to tainted websites loaded with viruses and malware 12.5 percent of the time. Also among the most dangerous women on the Internet are Eva Mendes, Halle Berry, Salma Hayek, and Sofia Vergara.

TIP

Don't click on links or download attachments unless you are absolutely sure that the source is legitimate. The risk is too great. Stick to legitimate websites with which you are familiar when looking for information about popular characters or people. Make sure that your security software, antivirus software, and anti-malware software are up-to-date with the latest patches.

Iron Man 3

The movie *Iron Man 3* was a huge worldwide hit in 2013. Pirated versions of movies distributed on the Internet are a major problem for the movie industry, but they are also a major problem for consumers. I don't condone buying cheap bootlegs of movies over the Internet; that is a crime. However, I understand that many people will be tempted to purchase or even get free what they think are pirated versions of popular movies. Identity thieves understand this too, which is why soon after the release of *Iron Man 3* there were more than a hundred websites, not connected with the studio that produced *Iron Man 3*, claiming that they had copies of *Iron Man 3* for purchase or free in some instances. These sites required you to download a file containing a video player. The problem is that by downloading this video player, you might have downloaded keystroke-logging malware along with or instead of the promised video player. This malware can steal all of your personal information from your computer, including credit card numbers, bank account numbers, and passwords, and turn you into a victim of identity theft.

TIP

Never click on links or download files unless you know that what you are clicking on or downloading is legitimate. Obviously, you cannot trust someone who is promising to provide you with a pirated product. The risk of downloading malware is just too great. Pay your money and go to the movie in the theater, or if you want a home version, it won't be too long before the movie is legitimately available online.

Nude Photos of Carla Bruni

The promise of nude photographs of Carla Bruni, the attractive wife of French President Nicolas Sarkozy, was used to phish into the computers of dozens of diplomats attending the 2011 Group of 20 economic summit. This group, generally referred to as the G20, is an organization of finance ministers and central

bank governors from 20 major world economies. The ministers each received an e-mail with the subject line being "French first lady nude photos" and containing a link to connect to those photos. According to a French government source, almost all the ministers and bank governors receiving the e-mail took the bait and clicked on the link, which indeed did take them to nude photos of Carla Bruni. However, by clicking on the link, the ministers and bank governors also unwittingly downloaded keystroke-logging malware that was used to steal information from the computers of those hacked. It is worth noting that before becoming the wife of Nicolas Sarkozy, Carla Bruni was a model, actress, and singer who often posed nude, and her nude pictures can be readily accessed on the Internet without the viewer having to click on tainted links. The goal of the hackers from China who perpetrated this crime was most likely to obtain important financial information from these ministers and governors. The promise of nude photos being used to lure people into clicking on tainted links is nothing new. Every year this type of scam catches many unwary people.

Debit Card Phishing Scam

Customers of St. Anne's Credit Union, BankFive, Bristol County Savings Bank, Mechanics Cooperative Bank, Taunton Federal Credit Union, and Bridgewater Savings Bank in Massachusetts received telephone calls purportedly from their banks in which the caller told the person answering the call that the caller worked for his or her bank, that there was a security breach of the customer's bank account, and that the account had been frozen for security purposes. The customer was then told that in order to resolve the situation and make the account available to the customer again, the customer had to confirm his debit card number and PIN (personal identification number). Of course, the calls were not coming from the customers' banks. They were coming from identity thieves seeking this information in order to access the accounts of the people receiving the calls. In truth, not only were the calls not coming from the banks, but many of them came from identity thieves who were not even located in the United States.

TIP

Your real bank will not ask for your debit card number or PIN on the phone. Whenever you get a telephone call, text message, or e-mail requesting such information, you should refuse to provide it because you can never be sure that the communication is legitimate. In fact, in all circumstances, this will merely be a scam attempting to get your personal information in order to make you a victim of identity theft. If you have any thought that the communication might be legitimate, call your bank at a number that you know is legitimate to inquire as to the status of your account.

Another Debit Card Phishing Scam

Another debit card scam involves victims receiving text messages purportedly from their bank telling them that their debit card had been deactivated and to call a telephone number provided in the text message to straighten out the matter. Victims who fall for this ploy call the number and are instructed to provide their debit card numbers and PINs. What makes the identity thief's initial communication appear to be legitimate is that it often contains the first four digits of your debit card. However, the first four digits do not relate to you individually, but are associated with the particular financial institution and its location. This information is easy to get. It is also important to remember that financial institutions will never ask for your debit card number or PIN. They already have this information.

Phishing with a Large Net

The Phishing Attack Trends Report is published monthly online at www.antiphishing.org by the Anti-Phishing Working Group, an organization dedicated to eliminating identity theft resulting from phishing. A recent monthly report stated that the companies most often imitated by phony phishing websites were eBay, Citibank, AOL, and PayPal.

Phishing Around the World

In an effort to clean up their own house, EarthLink, the Internet access provider, went on a phishing expedition of their own, trying to trace the purveyors of phony phishing schemes, and what they found was both startling and disturbing. Many of the phishing scams they were able to track originated in e-mails from around the world, particularly Russia, Romania, other Eastern European countries, and Asia. In Romania, Dan Marius Stefan was convicted of stealing almost half a million dollars through a phishing scam and was sentenced to 30 months in prison.

For every computer geek or small-time phisher, such as convicted identity thief Helen Carr, who used phony e-mail messages purporting to be from AOL to steal people's money, it appears that more sophisticated organized crime phishing rings are popping up, posing a serious threat to computer and smartphone users. This presents a growing problem for law enforcement.

Spearphishing

Most often phishing e-mails are not directed at you by name, but rather to you as "customer" or "consumer." They also might appear to come from companies with which you do not do business, such as a bank where you have no accounts.

However, with the epidemic of hacking of large companies and governmental agencies, many identity thieves are able to use the hacked information to send you a personal, phony e-mail that contains your name and is definitely from a company or agency with which you do business, making you more likely to respond to the urging to click on the dangerous link contained in the e-mail. This type of targeted phishing is called "spearphishing" and it is extremely dangerous.

Never click on links in e-mails unless you are absolutely sure they are legitimate. If you get a link-containing e-mail from a company with which you do business, you should always be skeptical and make sure that you call the company before considering clicking on the link to confirm whether the e-mail is legitimate. The mere fact that the e-mail uses your name and even your account number does not necessarily mean that the e-mail is legitimate.

How Do You Know That You Have Become a Victim of Phishing?

The problem is that you might not know that you have been a victim of identity theft through phishing. When a mugger takes your wallet, immediately you know that your money has been stolen; however, when an identity thief steals your identity through phishing, you might not remember what appeared to be the innocuous e-mail, text message, or website that started you on the road to having your identity stolen. As always, an ounce of prevention is worth a gigabyte of cure.

Reloading

Reloading is the name for the scam when scammers go back to victims of scams, identity theft, or hacking, purporting to provide assistance in straightening out the mess created when the victim was first harmed, when in fact, what the scammers are actually doing is getting more money out of the victim under the guise of helping the victim or getting more personal information from the victim that leads to further identity theft. This happened in response to the Target hacking. Although Target was legitimately contacting its customers by e-mails, so were identity thieves purporting to be either Target or a consumer protection agency. In both cases, the identity thieves attempted to lure the victims into clicking on links in the e-mails. These links either downloaded malware onto the victim's computer and permitted the identity thief to steal all the information from the victim's computer and lead to the person becoming a further victim of identity theft, or led to a page where the victim was prompted to provide personal information directly, which would lead to identity theft. In

other circumstances, the victim was told that he or she had to pay for assistance from the phony consumer protection agency.

No legitimate consumer protection agency such as the Federal Trade Commission or your local state attorney general's consumer protection division ever requires you to pay for their services. Never click on links in e-mails regardless of how legitimate the e-mails look until you have confirmed that they are indeed legitimate. In the case of Target, as with other companies, don't click on the links in their e-mails, but rather go directly to their legitimate website at an address that you know is accurate for further information. Also, do not provide personal information to anyone until you have confirmed that the person, company, or agency both is legitimate and has a real need for the information. Finally, make sure that your computer, laptop, tablet, and smartphone are all protected with the latest anti-malware software, and keep that software up-to-date.

Identity Theft Through Internet Phone Calls

Identity thieves have used unsolicited telephone calls in which they trick people into revealing personal information, such as credit card numbers or Social Security numbers, for many years. This has proven to be lucrative, but time-consuming. Now, however, some identity thieves are using modern technology such as automatic dialing software and Internet telephone services to make huge numbers of automated robocalls around the world in just a few moments. A typical scam using this technology involves a call purportedly from a person's credit card company telling him that his card needs to be reactivated and that the person receiving the call needs to punch in his credit card number. It is also important to note that some of these identity thieves also take advantage of a technique called "spoofing" by which the caller ID of the person receiving the call will appear to show a legitimate source for the call, such as the person's bank, when, in fact, the call is originating with an identity thief anywhere in the world.

It is easy to identify a scam robocall. All robocalls, with the exception of those from charities or politicians, are illegal, so if you receive one that indicates it is from your bank or a credit card company, it is a scam. In addition, when you receive a call, you can never be sure, regardless of what your caller ID might say, as to the identity of the person calling you; therefore, you should never provide personal information over the phone to anyone whom you have not called. If you do receive a call that appears to be legitimate requesting personal information, just hang up and call the real entity to find out whether the call was legitimate.

What Do Kim Kardashian and Michelle Obama Have in Common?

In 2013 Kim Kardashian, Kris Jenner, Ashton Kutcher, Paris Hilton, Joe Biden, Michelle Obama, Hillary Clinton, Bill Gates, Beyoncé, Mel Gibson, and FBI director Robert Mueller all became targets of identity theft, with Kris Jenner alone losing more than $70,000. Foreign hackers were able to steal the identities of 23 famous politicians, celebrities, and sports figures, including the aforementioned people, by hacking into the website www.annualcreditreport.com and getting access to their victims' credit reports. These reports provided a treasure-trove of personal information that, in the hands of an identity thief, could cause serious harm to the people whose information was stolen. Instead of quietly using this information as most identity thieves would do, these hackers publicized the information on the Internet, which is where identity thieves obtained this information and used it to steal from these victims.

Why this is important to you is that the initial hacker was able to get into his victims' credit reports due to a flaw in the authentication process at www.annualcreditreport.com. Without going into the details, the manner in which the security questions were set up made the system easy to crack, particularly when much of the information required to be furnished in order to answer the security questions and access the accounts could be found throughout the Internet. Certainly, public figures have much personal information available on the Internet for people to readily search out. You might think that you are not a public figure and that your personal information is not easily available, but think again. Too many people put too much personal information about themselves on social media, which then becomes fertile ground for someone trying to steal your identity. The lesson is that less is more. The less personal information you make available on social media, the more you protect yourself from identity thieves.

USB Sticks and Identity Theft

Curiosity killed the cat, and it can also invade your computer and result in an identity thief getting access to your computer through malware such as a keystroke-logging program that can read and steal all the information stored on your computer, such as your Social Security number, credit card numbers, and passwords. It can lead to your becoming a victim of identity theft. Identity thieves leave USB sticks in parking lots of companies that they want to hack, hoping that people who work there will see the USB sticks and then, being curious about what is on them, put them into their computers at work and unknowingly download the malicious software. Never put a USB stick that you are not absolutely sure is clean into your computer. The risk is too great. Let the cat live.

Internet of Things

As if we all didn't have enough to worry about, now we have the Internet of things about which to be concerned. More and more of the things we use are becoming connected to the Internet, including but certainly not limited to cars, refrigerators, coffee makers, and thermostats. It is tremendously convenient, for example, for us to use our smartphones to program our thermostats from afar so that our homes will have the proper temperature when we return from a day at work. But every technological advance, regardless of how constructive it might seem, has the potential to be exploited by scammers, hackers, and identity thieves. The Internet security company Proofpoint found that a botnet of more than 100,000 was made up of not only hacked computers but also (25 percent) Internet-connected devices including televisions and refrigerators. A botnet is a network of hacked electronic devices used by scammers and identity thieves to spread malware while avoiding detection.

The differences between computers and television sets have blurred in recent years, with many people buying Internet-connected high-definition televisions. Too often, people fail to recognize the security threats present in these new devices, much to their detriment. Hackers can breach your Internet-connected television and fool you into trusting phony bank or shopping websites, thereby making you a victim of identity theft. Fortunately, companies have developed security programs for Internet-connected television sets. Before you even consider buying an Internet-connected television set, you should make sure that you have it properly equipped with security software.

TIP

The danger posed by botnets of devices, part of the new Internet of things, is quite real and very chilling. Although many of us would not think of neglecting to provide proper security software for our computers, laptops, tablets, and smartphones, many people do not consider what they need to do to maintain the privacy and security of their refrigerator, car, and other devices that are a part of the new Internet of things. Unfortunately, among the people not giving enough attention to security in the Internet of things are the very companies developing these products. The most effective place to find a helping hand is at the end of your own arm, so whenever you are considering purchasing a convenient device with Internet capabilities, be sure to inquire as to the necessary security steps to take to make your use of the device safe.

What You Can Do to Prevent Identity Theft

As damaging as identity theft can be and as vulnerable as we are to identity theft, there are a number of relatively simple things you can do to make yourself less likely to become a victim of identity theft:

- Do a little spring cleaning in your wallet or purse even if it is the middle of summer. Do you really need to carry all the cards and identifications that you presently carry? In particular, don't carry your Social Security card in your wallet or purse. In the hands of an identity thief, it is the key to identity theft.
- If you rent a car while on vacation, remember to destroy your copy of the rental agreement after you have returned the car. Don't leave it in the glove compartment.
- Stolen mail is a ripe source of identity theft. When you are traveling, you might want to have a neighbor you trust pick up your mail every day or have your mail held at the post office until your return. Extremely careful people or extremely paranoid people, depending on your characterization of the same people, might prefer to use a post office box at the post office for receiving mail rather than a mailbox at home. Identity thieves also get your mail by filling out a "change of address" form using your name to divert your mail to them. If you find that you are not receiving any mail for a couple of days, it is worth contacting your local postmaster to make sure everything is okay. The U.S. Postal Service now requires post offices to send a "Move Validation Letter" to both the old and the new address whenever a change of address is filed. If you receive one of these notices and you have not recently changed your address, you should respond immediately because it could well be a warning that an identity thief has targeted you. A careful credit card user keeps an eye on his or her mailbox for the arrival each month of the monthly statement from the credit card company. If a bill is missing from your mail, it might mean that someone has hijacked your account and filed a change of address form with the credit card issuer to buy some more time. The sooner you are aware that the security of your account has been compromised, the better off you will be. You should also be particularly watchful of the mail when your card is close to expiration. An identity thief might be in a position to steal your mail containing your new card. If an identity thief is armed with enough personal information to activate the card, you could be in trouble.
- Prudent people might want to use travelers' checks while on vacation rather than taking their checkbook, because an enterprising identity thief who manages to get your checkbook can access your checking account and drain it.

- Be wary of who might be around you when you use an ATM (automated teller machine). Someone might be looking over your shoulder as you input your PIN. That same someone might lift your wallet shortly thereafter. Next step: disaster. In addition, ATMs are common targets for identity thieves who tamper with the machine by installing devices called skimmers that can read your card as you insert it into the machine. This information is then electronically transferred to the identity thief, who creates a duplicate of your card and is able to access your account. Never use an ATM if it appears in any way to have been tampered with, and always check for evidence of tampering in the slot where you insert your card. If it appears loose, go to another machine.
- Make copies of all of your credit cards, front and back, so that you can tell whether a card has been lost or stolen. Also keep a list of the customer service telephone numbers for each card. When copying your cards, you might also want to consider whether you really need that many cards.
- Be careful when storing personal information and mail, even in your own home. Louisiana police arrested a baby sitter on identity theft charges for stealing credit applications mailed to the people for whom she was baby sitting and for opening accounts using the Social Security number of her employer, which she obtained by rummaging through her employer's documents.
- After you have received a loan, a credit card, or anything else that required you to complete an application containing your Social Security number, request that your Social Security number be removed from the application kept on record. In addition, if you are feeling particularly paranoid (and it is important to remember that even paranoids have enemies), ask that your credit report used by the bank or other institution be shredded (cross shredded, remember?). They no longer need this information after you have received your loan. Holding your Social Security number in their data banks only serves to make you vulnerable to identity theft should the company suffer a data breach.
- Make life easier for yourself. Remove yourself from the marketing lists for preapproved credit cards and other solicitations. You can remove yourself from the Direct Marketing Association's solicitation list by writing to them at Mail Preference Service, Direct Marketing Association, P.O. Box 9008, Farmingdale, NY 11735. Include your name and address, but no other personal information. You can also take yourself off of the list of preapproved credit offers for five years by going online to www.optoutprescreen.com. Register for the Direct Marketing Association's Mail Preference Service to opt out of national mailing lists online at www.dmachoice.org. You can also print the form and get yourself removed from mailing lists. Additionally, at the same website,

you can also remove yourself from commercial e-mail solicitations. When you go to www.dmachoice.org, go to the Consumer FAQ page, where you will find the links to remove yourself from these mailing lists. DMA members are required to remove people who have registered with the Mail Preference Service from their mailings. However, because the list is distributed only four times a year, it can take about three months from the time that your name has been entered to see a reduction in junk mail. It is also important to remember that many spammers are not members of the Direct Marketing Association, so you can still expect to receive some spam e-mails as well as spam snail mail.

- If you do get unwanted spam e-mails, do not click on the "remove me" link provided by many spam e-mails. All you will succeed in doing is letting them know that you are an active address and you will end up receiving even more unwanted e-mails.
- If you receive spam faxes, you also should be wary of contacting the telephone number provided in many spam faxes to remove yourself from their lists. It is already illegal for you to have received a spam fax. Contacting someone who is already ignoring the law by having sent you the spam fax might cost you for the call and will not reduce your spam faxes.
- Sign up for the National Do Not Call Registry to reduce unwanted telemarketing calls. Most telemarketers are legitimate. Almost all are annoying and many are criminals setting you up for identity theft or other scams. To sign up for the Do Not Call Registry, you may call toll free 888-382-1222 or register online at www.donotcall.gov. Again it is important to remember that criminals pay little attention to the Do Not Call Registry, so it does not prevent identity thieves and scam artists from calling you. However, knowing that a telemarketer calling you is in violation of the Do Not Call Registry is a good indication that the caller is not worth listening to and you should hang up right away.
- Check your credit report at least annually, and remember to get copies from each of the three major credit-reporting bureaus, all of which independently compile the information contained in their files. Federal law permits you to annually obtain a free copy of your credit report from each of the three major credit-reporting agencies: Equifax, TransUnion, and Experian. You can get your free credit reports by going to www.annualcreditreport.com or by calling 877-322-8228. It is important to note that there are a lot of companies that appear to be offering free credit reports, but if you read the fine print (and rarely will you find anything fine in fine print), you might learn that when you sign up for your "free" credit report with one of these companies, you will have also signed up for a costly monthly service that you might

not have desired. A good indication that the offer to provide you with a free credit report is not "free" is when you are required to provide them with a credit card. Why would you need to provide a credit card number for a free service? The only official website from which you can truly obtain your credit reports free without any conditions is www.annualcreditreport.com. Be wary of websites with deceptively similar URLs. You also might want to consider staggering the obtaining of your credit reports by ordering one of your credit reports from each of the three major credit-reporting agencies every four months so that the information you are receiving is more current. Look over your file and make sure everything is in order. Particularly look for unauthorized and inaccurate charges or accounts. Also, check out the section of your report that deals with inquiries. A large number of inquiries that you have not authorized could be the tracks of an identity thief trying to open accounts in your name. A large number of inquiries can also have the harmful effect of lowering your credit score.

- Check your Social Security statement as provided by the Social Security Administration annually. It provides an estimate of your Social Security benefits and your contributions and can be helpful in detecting fraud. It is also a good thing to check this statement carefully each year to make sure that the information contained within it is accurate to ensure that you are slated to receive all the Social Security benefits to which you are entitled.
- Don't carry your Social Security card with you. You don't need it with you at all times, and if your wallet or purse containing your Social Security card is lost or stolen, you have handed over the key to identity theft to a criminal.
- Carefully examine your monthly bank and credit card statements for any discrepancies. This can be particularly important in limiting liability for the use of a stolen debit card.
- Carefully examine all medical bills and statements for services that you receive to make sure that medical charges are not being made for services received by someone else using your medical insurance.
- Never give personal information on the phone to someone you have not called. You can never be sure of the real identity of anyone who calls you. Even if you have caller ID and it seems to indicate that the call is legitimate, such as appearing to come from your bank, it might not be legitimate. Identity thieves are able to "spoof" legitimate numbers so that the number that appears on your caller ID appears legitimate when, in fact, it is not the real number calling you. If you believe that the call might be legitimate, merely hang up and call the company back at a number that you are sure is the correct and legitimate number.

- Protect your computer with a strong password as well as a proper firewall and with antivirus and anti-malware security software, and make sure that it is automatically updated.
- Protect your smartphone and other portable devices with security software and complex passwords.
- Shred, shred, shred any documents that you intend to discard that contain any personal information. Make sure that you use a cross shredder because vertically shredded material can be reconstructed by identity thieves. Although the IRS has up to six years in which to audit your income tax return if they allege you underreported your income by at least 25 percent, you are probably safe shredding income tax returns and supporting records after three years, the normal period for the IRS to perform an audit. Credit card statements, canceled checks, and bank statements should be shredded after three years.
- When doing any financial transactions on your computer, laptop, smartphone, or other electronic device, make sure that your communications are encrypted. This is particularly important if you are using public Wi-Fi.
- Don't share your passwords with anyone. Trust me, you can't trust anyone. Make sure that you use complicated passwords that are not something easily identified with you, such as your pet's name.
- Limit the information you share on social networking sites in order to make it more difficult for identity thieves to access personal information that can be used to make you a victim of identity theft.
- I know it is boring, but read the privacy policies of any websites you use where you provide personal information. Make sure you know what they do with your personal information, whether they share it with anyone, and how they protect it. What you read might surprise you and it might influence you to avoid that particular website.
- Not all of your personal information is on your computer and not all identity thieves come from Nigeria. Sometimes they are relatives, neighbors, or anyone else who might have access to your home and access to your personal records that might contain your Social Security number or other important personal information. Keep your personal and financial information documents locked and secure at home.

Index

Q-R

S

T