50 WAYS TO PROTECT YOUR IDENTITY IN A DIGITAL AGE

NEW FINANCIAL THREATS YOU NEED TO KNOW AND HOW TO AVOID THEM

STEVE WEISMAN

Praise for the First Edition of *50 Ways to Protect Your Identity*

"The author substitutes straight talk for legal mumbo-jumbo in *50 Ways to Protect Your Identity*. Reading this book is like getting a black belt in consumer self-defense."

—Jim Bohannon, host of *The Jim Bohannon Show*

"Identity theft is among the fastest-growing problems facing Americans today. This book will help you learn all you need to know to protect your lives, money, and security. Consider it your first stop in your quest for knowledge and guidance to prevent ID theft."

—Robert Powell, Editor of CBS *MarketWatch*

"As one who has lived through some of the nightmare scenarios discussed by the author, I believe 'Steve's Rules' need to be placed in a prominent place so you can see them any time you think you are safe. They may be the new practical commandments for financial survival."

—Doug Stephan, host of the *Good Day* **nationally syndicated radio show**

"Detecting and stopping identity thieves is imperative to protecting your finances and financial reputation. Steve Weisman shows you how to protect yourself and what steps to take if you are victimized. This is a must-read for anyone with a bank account and a credit card!"

—Bonnie Bleidt, Boston Stock Exchange Reporter, CBS4 Boston, Host of *Early Exchange***, WBIX**

This page intentionally left blank

50 Ways to Protect Your Identity in a Digital Age

Second Edition

This page intentionally left blank

50 Ways to Protect Your Identity in a Digital Age

New Financial Threats You Need to Know and How to Avoid Them

Second Edition

Steve Weisman

Vice President, Publisher: Tim Moore
Associate Publisher and Director of Marketing: Amy Neidlinger
Executive Editor: Jim Boyd
Editorial Assistant: Pamela Boland
Operations Specialist: Jodi Kemper
Marketing Manager: Megan Graue
Cover Designer: Chuti Prasertsith
Managing Editor: Kristy Hart
Project Editor: Betsy Harris
Copy Editor: Cheri Clark
Proofreader: Sarah Kearns
Indexer: Lisa Stumpf
Compositor: Nonie Ratcliff
Manufacturing Buyer: Dan Uhrig

Publishing as FT Press
Upper Saddle River, New Jersey 07458

Printed in the United States of America

First Printing October 2012

ISBN-10: 0-13-308907-X
ISBN-13: 978-0-13-308907-3

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 Cataloging-in-Publication Data

Weisman, Steve.
50 ways to protect your identity in a digital age : new financial threats you need to know and how to avoid them / Steve Weisman.—2nd ed.
p. cm.
ISBN 978-0-13-308907-3 (pbk. : alk. paper)
1. Identity theft—United States—Prevention—Handbooks, manuals, etc. 2. Consumer credit—United States—Handbooks, manuals, etc. 3. Credit ratings—United States—Handbooks, manuals, etc. 4. Privacy, Right of—United States—Handbooks, manuals, etc. 5. Records—Access control—United States—Handbooks, manuals, etc. I. Title. II. Title: Fifty ways to protect your identity in a digital age.
HV6679.W44 2012
332.024—dc23

2012028627

This book is dedicated to Jeanne and Arnie Weisman

This page intentionally left blank

Contents

Acknowledgments

So many people have encouraged me and supported me, not only in this book, but in my efforts to educate the public about the dangers of identity theft. I would like to take this opportunity to recognize a few of them:

Marc Padellaro, who inspires me in so many ways

Ron Nathan, an always supportive friend

Tom Mullen, who unselfishly helped me so much at a time I really needed his help

Michael Harrison, a great friend who also has provided continuing insights

And of course my wife, Carole, who is always by my side making my days and nights better

About the Author

Steve Weisman hosts the radio show *A Touch of Grey*, syndicated to 50+ stations nationwide, including WABC (NYC) and KRLA (LA). A senior lecturer at Bentley College, he is a member of the National Academy of Elder Law Attorneys and is admitted to practice before the U.S. Supreme Court. The legal editor for *Talkers Magazine* and a monthly columnist for the American Institute of Economic Research, 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.

This page intentionally left blank

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 halfway 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 always wondered how that worked. He said that he had too, and 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.

1

Identity Theft

Maybe Shakespeare was right when he said in Othello, "Who steals my purse steals trash; 'tis something, nothing;...but he that filches from me my good name robs me of that which not enriches him, and makes me poor indeed."

Let's say you are at a car dealership and the salesman comes back with a long face and tells you the financing on the car you wanted to buy has been turned down, or the dealership has had to go to another loan source that means higher interest and payments. "But I have great credit," you say.

In another scenario, you apply for another credit card and are turned down. In both cases, you are shown a copy of your credit report and find late-payment notices or applications for credit cards in other cities. *Someone has stolen your identity.*

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; 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.

Consumer Sentinel Network

The Consumer Sentinel Network is a government organization that collects millions of consumer complaints available only to law enforcement. According to its most recent data, identity theft is the number-one consumer complaint. Government documents/benefits fraud was the most common form of identity theft reported, credit card was the second most common form of identity theft, and phone and utilities fraud was the third most common form of identity theft, followed by bank fraud identity theft and loan fraud identity theft.

The President's Identity Theft Task Force

According to the President's Identity Theft Task Force report in 2007, billions of dollars are lost to identity theft each year, and this number has only gone up since the report was first issued. Victims of identity theft find themselves sued by creditors of the people who stole their identities. The time, money, and effort that it takes to repair the harm done by identity thieves can be tremendous.

According to the Task Force report, identity thieves are a varied group. They include people who had never before committed a crime, career criminals, and family members, as well as organized crime both here and abroad.

The report noted, "Identity theft is prevalent in part because criminals are able to obtain personal consumer information everywhere such data are located or stored. Homes and businesses, cars and health-club lockers, electronic networks, and even trash baskets and dumpsters have been targets for identity thieves. Some thieves use more technologically advanced means to extract information from computers, including malicious-code programs that secretly log information or give criminals access to it."

FTC Survey

According to a survey of the Federal Trade Commission, 27.3 million Americans were victims of identity theft within a five-year period. Fifty-two percent of identity theft victims first learned that they had been

victimized by monitoring their own accounts. Twenty-six percent of victims first learned from credit card issuers, banks, or other companies with which they did business that they had been the victims of identity theft; 8 percent of the victims first found out that their identity had been stolen when they applied for credit and were turned down. The survey also revealed that most identity thieves use personal information to buy things; however, 15 percent of all victims were victimized in non-financial ways, such as when an identity thief used the victim's identity when apprehended for another crime by police. Sixty-seven percent of identity theft victims found that their existing credit card accounts were improperly accessed, and 19 percent of identity theft victims said that their checking or savings accounts had been looted.

According to the Consumer Sentinel Network Data Book for the year 2011, the state with the highest number of identity theft victims proportionate to its population was Florida, followed by Arizona and California. North Dakota had the fewest number of complaints of identity theft, with only 23.2 complaints for every 100,000 people in 2011. The report also ranked identity theft as the number-one consumer complaint for each of the past 12 years.

The FTC has been helping identity theft victims since 1998 and has an excellent Identity Theft Program to help victims and provide information to help combat this problem. If you are the victim of identity theft, you can file a complaint with the FTC by calling 1-877-IDTHEFT (438-4338) or going online at www.ftccomplaintassistant.gov. When a complaint is made, the information is stored and made available to law enforcement agencies around the country. Victims should not be concerned that the information will make them susceptible to further identity theft; the database is safe and secure.

2012 Javelin Strategy & Research Report

According to Javelin Research, identity theft worsened by 13 percent in 2011 with increased numbers being associated with increased use of social media and smart phones and other portable electronic devices as well as a startling 67 percent increase in the number of Americans affected by data breaches.

Immigration Fraud

It is common for illegal immigrants to buy Social Security numbers of identity theft victims on the black market in order to get a job. Victims of this type of identity theft might find themselves mistakenly identified as an illegal alien or have their own government benefits, such as Social Security benefits, compromised.

It Can Happen to Anyone

In 2012, an AWOL soldier, Brandon Lee Price, was arrested and charged with stealing the identity of Microsoft cofounder Paul Allen. According to the FBI, Price called Citibank in January of 2012 and changed the address on a bank account of Allen's from Seattle to Pittsburgh; then a few days later, he requested a new debit card for the account after stating that he had lost his debit card. Price used the card to access Allen's account and pay off his own outstanding debts.

A Big Problem

Frank Abagnale is a former identity thief who has left, as they say in *Star Wars,* the dark side of the force and is now a recognized expert on personal security matters. His exploits were described in his book, *Catch Me If You Can,* which was later made into a hit movie starring Leonardo DiCaprio and Tom Hanks.

In an interview with bankrate.com, he spoke about one of the major problems in fighting identity theft: "Visa and MasterCard have losses amounting to $1.3 billion a year from stolen, forged, altered cards, or those applied for under false pretenses. In the end they will probably raise fees and service charges to recoup these losses."

Abagnale went on to say, "Banks and corporations have found it is easier to write off a loss than it is to prosecute it. Most district attorneys have a benchmark set and do not prosecute forged checks under $5,000. Most U.S. attorneys have a benchmark of $250,000 before prosecuting white-collar crimes, and the FBI is under a directive not to investigate crimes under $100,000. The problem for the government agencies and

municipalities is the lack of manpower and resources to prosecute these crimes."

Treasury Secretary John W. Snow on Identity Theft

In a speech in June of 2003, Treasury Secretary John W. Snow said, "The wretched depravity of some identity crimes defies the imagination. In a ring stretching from New Jersey to California, a healthcare worker in cahoots with bank insiders and mortgage brokers got the names of terminally ill hospital patients, forged their identities, drained their bank accounts, and then bought houses and cars in their names—stealing their identity and looting their finances. Another recent case involved a rash of scammers posing in military uniforms who visited the wives of soldiers deployed in Iraq. They falsely informed the wives that their husbands had been seriously wounded. The con artists then tried to collect personal information about the soldiers from the distraught wives, to enable the scammers to use the soldiers' identities and steal the families' savings."

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 misuse, 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 the 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 mujahadin 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."

Patriot Act

A particularly insidious identity theft scam used the Patriot Act as a ruse to get your personal financial information. Again, it started with an e-mail, this time purporting to be from the Federal Deposit Insurance Corporation (FDIC), which said that then Department of Homeland Security Director Tom Ridge had notified the FDIC to suspend all deposit insurance on your bank accounts due to possible violations of

the Patriot Act. After luring you into the trap, the criminal sending the e-mail then indicated within the e-mail that all your FDIC insurance would be suspended until you provided verification of personal financial information, such as your bank account numbers.

WARNING

The FDIC does not send out e-mails for these purposes. Never provide personal financial information over the Internet unless you have initiated the contact and you are absolutely sure of who you are dealing with.

What Do Identity Thieves Do?

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

- Gaining access to your credit card account, bank account, or brokerage account
- 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
- Buying cellphones in your name
- Using your name and credit to pay for utilities, such as fuel oil or cable television
- Using your medical insurance to obtain medical services, thereby corrupting your medical records
- Renting a home
- Using your name when committing crimes

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

NOWHERE ARE YOU SAFE

In November of 2003, in Virginia, an emergency medical technician was arrested and charged with credit card theft, credit card fraud, attempted grand larceny, and identity theft stemming from an incident that occurred when the EMT was called to a nursing home to assist an 80-year-old resident. While going through her purse for identification, he took one of her credit cards. When he returned to the fire station, he went online using the fire department's computer to order a 42-inch plasma television paid for with the stolen credit card. Fortunately, the credit card company was vigilant and flagged this unusual purchase for an elderly nursing home resident. They called the victim's daughter who managed her mother's financial affairs. She promptly told the credit card company that it was a mistake. It did not take Sherlock Holmes to identify the villain because the stupid thief gave the address of the fire station as the delivery address for the television. Due to prompt action in investigating the matter, the television never was delivered. The computer provided further information that led to identifying the EMT who had helped himself to his victim's identity.

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. Go to any post office and inevitably you will find in their trash containers much of this material that owners of post office boxes toss out when they go through their mail before they even 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 debts in the victim's name.

YOU ARE ONLY AS SAFE AS THE PLACES THAT HAVE YOUR INFORMATION

No matter how careful you are about protecting your personal information from identity thieves, you are only as safe as the places that have 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 its customers or members and either use it themselves for identity theft purposes or sell the information to professional identity thieves.

HACKERS

Computer hacking of government and private business computers have resulted in the personal information of millions of people being compromised. The Secret Service reported in the President's Identity Theft Task Force report of 2007 that major breaches in America's credit card systems were done by hackers from the Russian Federation and the Ukraine.

As the old cartoon character "Pogo" once said, "We have met the enemy and he is us." As more and more of us make greater use of our smartphones, iPads, and other portable electronic devices, people who make sure that their home computers are equipped with proper security software fail to do so with their portable electronic devices, and identity thieves are constantly exploiting this weakness.

NO CURE FOR STUPID

According to comedian Ron White, "There is no cure for stupid." Sometimes personal information is handed to identity thieves merely by the stealing of laptops or other portable electronic devices containing unencrypted personal information. The President's Identity Theft Task Force report gave the example of computers stolen with data on 72,000 Medicaid recipients in 2006.

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 utilized for identity theft. Methamphetamine addicts are perfectly suited for 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.

Phishing—Go Phish

You might remember the commercials by Citibank about its identity theft protections in which the voice of a young woman describing the bustier she bought with her credit card comes out of the body of an overweight, slovenly man. The ads made their point, but unfortunately so did the identity thieves who targeted Citibank and other companies through a tactic known as "phishing," in which they sent e-mails to unsuspecting consumers telling them that they needed to click on a hyperlink to update their information with the companies. When unsuspecting victims clicked on the hyperlink, they came to a Web site that looked like the real McCoy, or Citibank for that matter, but it was a phony. When the consumer entered his or her personal information, such as Social Security number or a credit card number, the identity thief had all he or she needed to either use the information to steal the identity of the victim or sell the information to other thieves. In the last two months of 2003, Citibank issued 14 alerts to its customers warning them of this dangerous scam.

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 the

unwary victim's passwords in order to stay online on someone else's dime. After a while, this phony fishing expedition, fishing for information, came to be known as "phishing."

Phishing with a Pal

PayPal is a company with which anyone who has ever bought something on eBay is familiar. PayPal is an online payment service, owned by eBay, used to securely transfer money electronically. Through the popularity of eBay's online auction site, PayPal has gathered 40 million customers who use its services to make sure that the exchange of funds for auctioned items is done safely and securely. But for many people, that safety and security are an illusion. Through phishing, a con man sets up a Web site that imitates a legitimate Web site, such as PayPal, but whose sole purpose is to obtain sensitive personal financial information that can be used to facilitate identity theft. With the computer and software technology so readily available to pull off such a crime, the skill and artistry of the forgers of yesterday are not needed by the identity-stealing phishers of today.

Through phony e-mails that looked as though they were from PayPal, the identity thieves contacted retailers that used PayPal's services and requested confirmation of their passwords and other account information. According to PayPal, the passwords requested provided the criminals with access to sales information, but fortunately the personal financial information of their customers is stored on separate secure computer servers that are inaccessible to merchants or others that use PayPal's services. That is the good news. The bad news is that, armed with customers' names and other information about their previous purchases obtained through this scam, the con men were in a position to contact the customers directly and trick the unwary customers into revealing personal financial information that opened the door to identity theft. In the past, con men have sent e-mails purporting to be from PayPal, telling the customers that their accounts would be put on a restricted status until they completed a credit card confirmation that could be found on the PayPal site to which the e-mail directed the consumer. Unfortunately, the Web site to which the consumers were directed was a phony site used by the criminals to phish for victims. Previously, criminals would just randomly send out millions of e-mail

messages, hoping to snag a few unwary victims. However, armed with personal account information surreptitiously obtained from PayPal using merchants, the phony e-mails would appear more legitimate and thus they were more likely to take in more victims.

WARNING

PayPal never asks for personal financial information by way of e-mail and never refers to previous transactions through e-mail. If you get such an e-mail, do not reply to it, but inform PayPal by telephone directly of the e-mail message you received.

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, it indicated that it was phony. The e-mail addresses of legitimate companies are usually simple and direct. Unfortunately, this is no longer the case. Now computer-savvy identity thieves are able to mimic the legitimate e-mail addresses of legitimate companies.

Two Things to Look For

When identity thieves mimic a legitimate company's e-mail address using the latest technology, there will be no SSL padlock icon in the lower corner of your browser. SSL is the abbreviation for Secure Sockets Layer, an Internet term for a protocol for transmitting documents over the Internet in an encrypted and secure fashion. In addition, when you type a different URL (the abbreviation for Uniform Resource Locator, the address of material found on the World Wide Web) into what appears to be the address bar, the browser's title will not change from the phony "welcome message."

More Good Advice

Don't fall for the bait. It takes a few moments 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 Web site, do not click on the hyperlink in the e-mail that purports to send you to the company's Web site. Rather, type in what you know to be the proper Web site 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 now using Internet search engines, such as Google and Bing, to lure people into clicking on links that people think will send them to a legitimate Web site, but that instead will download dangerous malware to their computer that can steal all the information on their computer and make them a victim of identity theft. Identity thieves have been able to infiltrate search engines by adapting their phony Web sites that contain the dangerous links 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 Web sites are tied to celebrity news or major world news events. If you are searching for such information, limit your searches to Web sites 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 Web sites 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.

Who Do You Trust?

The late Johnny Carson used to host a television show titled *Who Do You Trust?* If there are any English teachers reading this, they know it should have been "Whom Do You Trust," but why quibble? I bring up this trip down memory lane because if there is anyone people do trust, it is FBI director Robert Mueller. Consequently, when you receive an

e-mail from him endorsing the legitimacy of a particular lottery or notifying you of a possible inheritance, you might be considering trusting the e-mail. Don't. Despite the fact that the e-mails look quite official, with photographs of Director Mueller, the FBI seal, and other legitimate-looking trappings, the e-mails are always scams. Sometimes they ask for personal information for various reasons and sometimes they provide links for you to click on.

TIP

The FBI does not endorse lotteries or inform you of inheritances. The FBI will not be sending you e-mails asking for personal information. Any links you click on contained in such e-mail will most likely contain malware that will steal the information from your computer and make you a victim of identity theft. If you do get such an e-mail, the best thing you can do is to either ignore it or forward it to the real FBI.

AOL Scam

In a phishing case brought by the FTC and the Justice Department, it was alleged that Zachary Keith Hill sent out e-mails to consumers that looked as though they were from America Online. The e-mail address of the sender indicated that it was from the billing center or account department, and the subject line contained a warning such as "AOL Billing Error Please Read Enclosed Email" or "Please Update Account Information Urgent." The e-mail itself warned the victim that if he or she did not respond to the e-mail, his or her account would be canceled. The e-mail also contained a hyperlink to send unwary consumers to a Web page that looked like an AOL Billing Center. But it was a phony Web page operated by Hill. At the Web page, the victim was prompted to provide information such as Social Security number, bank account numbers, and bank routing numbers, as well as other information. Hill, in turn, used this information to facilitate identity theft. The FTC eventually settled its charges against Hill, who agreed to refrain from ever sending e-mail spam or setting up fictitious and misleading Web sites. As with just about all FTC settlements, Hill did not admit to violating the law, but he did promise not to do it again.

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 Web sites were eBay, Citibank, AOL, and PayPal.

Phishing Around the World

In an effort to clean up its own house, EarthLink, the Internet access provider, went on a phishing expedition, 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 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 users. This presents a growing problem for law enforcement.

NATIONAL DO NOT E-MAIL REGISTRY

The National Do Not Call Registry administered by the Federal Trade Commission has been a boon to many people who do not want to be annoyed by telemarketers. It would only seem logical that a national do not e-mail list would offer similar benefits to people wanting to avoid spam, the commonly used term for junk e-mail. It might seem logical, but there is no law providing for such a list. When you see a solicitation to sign up for a "National Do Not E-Mail Registry," what you are actually seeing is another phishing expedition seeking to snare your personal information and steal your identity. Don't fall for it.

How Do You Know That You Have Been 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, you know right away that your money has been taken, but when an identity thief steals your identity through phishing, you might not remember what appeared to be the innocuous e-mail that started you on the road to having your identity stolen. As always, an ounce of prevention is worth a gigabyte of cure.

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 that you can do to make yourself less likely to become a victim of identity theft:

1. Do a little spring cleaning in your wallet or purse, even if it is the middle of the summer. Do you really need to carry all the cards and identifications that you presently carry?
2. 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.
3. 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 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 you are not receiving any mail for a couple of days, it is worth contacting your local postmaster to make sure everything is okay. A recent preventive measure instituted by the U.S. Postal Service 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 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 holder keeps an eye on his or her mailbox for the arrival each month of his or her monthly statement from the credit card company. If a bill is missing, 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 become 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.

4. 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.

5. 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 (personal identification number). That same someone might lift your wallet shortly thereafter. Next step—disaster.

6. Make copies of all 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 want to consider whether you really need that many cards.

7. Be careful when storing personal information and mail, even in your own home. Shreveport, Louisiana, police arrested a baby sitter on identity theft charges. They alleged that she stole a credit application mailed to the people for whom she was baby-sitting and also opened other accounts using the Social Security number of her employer that she had found while rummaging through their documents.

8. 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, ask that your credit report used by the bank or other institution be shredded in your presence. They no longer need that information after you have received the loan.

9. 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 card 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.dmaconsumers.org, but there is a $5 charge for doing so if you do it online. You also can print out the form and get yourself removed from mailing lists at no cost. Additionally at the same Web site, you can also remove yourself from commercial email solicitations. When you go to www.dmaconsumers.org, go to the Consumer FAQs 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 get some spam emails and snail mail.

10. 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.

11. If you receive spam faxes, you also should be wary of contacting the telephone number to remove yourself from their lists. It is already illegal for you to have received the spam fax. Contacting the sender by its telephone removal number might cost you for the call and will not reduce your spam faxes.

12. 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. To sign up for the Do Not Call Registry, you may call toll free 888-382-1222 or register online at www.donotcall.gov.

13. Check your credit report at least annually and remember to get copies from each of the three major credit report 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 will see that often when you sign up for a "free" credit report, you have also signed up for a costly monthly service to follow. The only official Web site from which you can truly obtain your credit reports for free without any conditions is www.annualcreditreport.com. You also might want to consider staggering the obtaining of your credit reports by ordering one of your free credit reports from each of the three major credit-reporting agencies every four months so that the information you receive 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.

14. 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.

15. 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 is lost or stolen, you have handed over the key to identity theft to a criminal.

16. 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.

17. 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.

18. Never give personal information on the phone to someone you have not called. You never can be sure of the identity of a telemarketer or anyone who solicits you on the phone.

19. Protect your computer with a proper firewall and with security software that automatically is updated.

20. Protect your smartphone or other portable electronic devices with security software and good passwords.

21. Shred, shred, shred any documents that you intend to discard that have any personal information on them. Make sure you use a cross shredder because straight-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%, 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.

22. When doing any financial transactions on your computer, laptop, or smartphone, make sure that your communications are encrypted. This is particularly important if you are using public Wi-Fi.

23. Don't share your passwords with anyone, and make sure you use complicated passwords that are not something easily identified with you, such as your pet's name.

24. Limit the information you share on social networking sites in order to make it more difficult for identity thieves to access your personal information that can be used to make you a victim of identity theft.

25. I know it is boring, but read the privacy policies of any Web sites you go to on which 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 Web site.

26. 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 information. Keep your personal and financial information documents locked and secure at home.

This page intentionally left blank

2

Making Yourself Less Vulnerable to Identity Theft

Identity thieves believe that they deserve a lot of credit. Unfortunately, the credit to which they are convinced they are entitled is yours. Credit cards present an all-too-easy target for identity thieves. Protecting your credit cards from identity theft should be a priority for everyone. Take the following steps to reduce your chances of being the victim of credit card fraud:

1. Sign your credit card as soon as you receive it, and activate it. Some people believe that instead of signing your credit card, you should write "See ID" on the signature line on the back of the card. The hope is that whenever your card is used, the clerk or whoever is processing your purchase will check your ID to make sure that you are the one using your credit card. It sounds like a good idea, but credit card issuers are in general agreement that it is best to sign your card. Under the rules enforced between merchants and the major credit card issuers, such as Visa, MasterCard, and American Express, a merchant is supposed to compare the signature on the sales slip with the signature on the credit card. The merchant should refuse to go through with the transaction if the cardholder refuses to sign his or her card.
2. As much as possible, do not let your credit card out of your sight when you make a purchase; a significant amount of credit card fraud occurs when the salesperson with whom you are dealing, out of your view, swipes your card through a small apparatus called a "skimmer" that gathers all the information embedded in your card. The thief then uses that information to make charges to your account. Skimmers can also be unobtrusively installed on

ATMs, gas pumps, and any other machine through which you swipe your card. Always check any ATM or other machine for tampering before inserting your card.

3. Save your receipts and ultimately destroy those receipts by shredding.
4. Never give credit card information over the phone to anyone unless you have initiated the call.

ONLINE SHOPPING CREDIT CARD PROTECTION

The opportunities for identity theft during online shopping are magnified. Two ways of reducing the odds are through the use of either a single-use card number provided to you by your card issuer or by the establishment of a password to be used when your credit card is used online.

The single-use authorization number is tied to your credit card, but has a distinct one-time effectiveness so that even if the number is compromised, your credit remains safe from identity theft.

Even less bothersome to a regular online shopper is the use of a password that you set up with your credit card issuer. When you enter your credit card number during an online purchase, a pop-up box will appear, requesting your password. After you enter the password, the transaction continues. As further security, the Internet retailer with which you are dealing never sees or has access to your password. So even if the retailer's security is breached, your credit card is safe.

More and more people are doing their online shopping on their smartphones and other portable devices. Unfortunately, many people are not vigilant in protecting the security of their smartphones and portable devices through proper updated security software, and identity thieves are well aware of this fact. One way that identity thieves get access to your smartphone is through corrupted free apps that you download that contain keystroke-logging malware that can read all the information contained in your smartphone or other device, including credit card numbers.

TIP

Download apps only from official app stores such as iTunes. Even then, read reviews before downloading them, and make sure that your smartphone and other personal electronic devices are properly protected with regularly updated security software.

Lottery Scams

Let's face it. Winning a lottery is difficult enough, but it certainly is made more difficult if you have not even entered, which is why when you are notified that you have won a lottery that you did not enter, you should be skeptical. You should be even more skeptical if the e-mail message informing you of your good fortune asks for some personal information from you, such as a bank account number. It's a scam, and its sole purpose is to make you the victim of identity theft. Some phony lotteries will tell you that they need you to pay them for the income taxes on your prize. Although it is true that legitimate lottery winnings are subject to income taxes, either those taxes will be withheld from your prize before you receive your payment or you will be responsible for making the tax payment directly to the IRS. No legitimate lottery collects the income tax due from you.

Vote for Me

Identity thieves are both inventive and knowledgeable of the times. During a recent period when many political organizations were busy encouraging and assisting people in registering to vote, identity thieves were also being heard from. In Midway, Florida, identity thieves posing as members of legitimate political organizations went door-to-door pretending to assist residents in registering to vote, but were actually gathering personal information such as Social Security numbers to use for identity theft.

STORIES AND WARNINGS: ENTERPRISING INMATES

Although it certainly does not qualify as rehabilitation, the conviction in 2003 of James Sabatino of wire fraud does show that some prison inmates are doing more with their time than just sitting around watching television. James Sabatino was serving a 27-month sentence for threatening federal prosecutors when he managed to steal the identities of a number of prominent business executives and use the information gathered through these identity thefts to purchase close to a million dollars' worth of goods and services, all the while serving his prison sentence. It takes time to steal that much stuff, and Sabatino spent about eight hours a day on the phone committing his crimes. During the course of one month alone, Sabatino placed a thousand telephone calls from his cell (I expect he used a cellphone—all puns intended). In fact, Sabatino used his cellphone to order more cellphones from Nextel using the identity of a Sony Pictures Entertainment executive. The phones were sent to a phony Sony address (try saying that out loud) that in actuality was a Federal Express office where an accomplice retrieved the phones. Sabatino's ultimate undoing began when an alert executive at Sony, Jack Kindberg, received invoices for the purchase of 30 cellphones he had never ordered. Corporate security eventually traced the thievery to James Sabatino, who pleaded guilty to wire fraud and was sentenced to more than 11 years in prison. Maybe Sony Pictures will make a movie out of his story.

Do Not Call

You might be like me and were thrilled to sign up for the national do-not-call registry to make your telephone off limits to telemarketers. However, as an example of how everything is an opportunity for con men, a recent scam involves your being called by someone purporting to be from either your state's do-not-call list or the National Do Not Call List who asks you to verify some personal information for the list. Again, there is no reason why anyone operating a do-not-call list needs any information other than your telephone number. Remember Steve's Rule number one: Never give out personal information to anyone over the phone whom you have not called, and always be sure of to whom you are speaking.

Cellphone Cameras

Everyone uses the camera function of their cellphones. They are easy to use. They are also easily and often used by identity thieves to photograph your credit card or your PIN (personal identification number) and then use the information gained to steal your identity. In 2011, John Sileo, an expert on identity theft and fraud, was on a business trip to Orlando, Florida, to give a speech to the Treasury Department about avoiding identity theft. He took the opportunity to take his daughter to Disney World while he was in Orlando. Upon returning to his hotel room after a day with his daughter at Disney World, he was informed by his bank that his credit card had been compromised and someone had stolen his identity and purchased $3,000 worth of goods online. Sileo believed that it was someone using a cellphone camera who took a picture of his card when he used it at Disney World's electronic ticket booth.

A Danger in the Workplace

According to the research of Professor Judith Collins of Michigan State University, approximately 70% of all identity theft can be traced back to employees stealing personal information. As long ago as April 25, 2002, the Office of the Comptroller of the Currency, a part of the United States Treasury Department, sent a warning to all national banks in which it alerted banks to the activities of organized gangs of criminals who infiltrated banks through their tellers in order to perform identity theft and other crimes.

INSIDE JOB

In February of 2004, Thoung Mong Nguyen was sentenced to 12 years in prison and ordered to repay $1.3 million for operating an identity theft ring in which stolen credit card numbers and phony IDs were used to make purchases charged to their victims. A rogue employee of the Bank of America provided Nguyen with personal information such as Social Security numbers belonging to customers of the bank. This information was used to obtain driver's licenses and credit cards that were used by the criminals for fraudulent purchases.

Identity Theft and the ATM

If an identity thief uses your ATM card or debit card, the federal Electronic Fund Transfer Act provides you with some protection. The amount of your protection, however, is significantly affected by how fast you notify the bank that you have been victimized. The maximum amount for which you can be held responsible for a stolen debit card is $50 if you notify the bank within two business days of learning that your card has been lost or stolen. If you delay notifying your bank more than two business days after discovering that your card has been lost or been used improperly, but within 60 days of receiving a statement showing that the card has been used for an unauthorized transaction, the maximum amount of your personal financial responsibility for the misuse of the card is $500. But if you wait more than 60 days after learning of the unauthorized use, you stand to lose everything that was taken from your account between the end of the 60-day period and the time that you reported your card was missing. It is best to notify your bank by telephone first and then immediately follow up your call with a written notification. A sample notification letter can be found in Chapter 21, "Form Letters." It is important to note that, regardless of the law, both Visa and MasterCard have taken the consumer-friendly action of limiting their customers' liability for unauthorized debit card use to $50, regardless of the time it takes the customer to notify the bank.

A Primer on ATM Identity Theft

As bank robber Willie Sutton said, he robbed banks because that is where the money is. That also explains the attraction to identity thieves of automated teller machines. ATMs offer an easy way to use identity theft to steal people's money. The plain, hard fact is that ATMs are vulnerable. There are a number of ways to steal money through an ATM.

Not all ATMs are owned by banks. Private individuals, who are able to earn significant fees for ATM use by their customers, own many ATMs. To set up a private ATM business, one needs an ATM, sufficient money to stock the machine, and a bank account into which the ATM card user's bank can send the funds necessary to reimburse the ATM-owning businessman for the money withdrawn and the use fee. There are no government regulations or licensing requirements. The banking

industry itself sponsors independent service organizations that control the connecting of the privately owned machines to the bank networks. These independent service organizations, or ISOs, are intended to investigate and approve new private ATM owners, but the oversight is not particularly strong.

The owner of a privately owned ATM can install a mechanism within the machine that takes down and stores the account numbers and personal identification numbers of the people using the machine. The ATM-owning identity thief then just harvests the names, account numbers, and PINs and uses that information to steal money from the bank accounts of unwary victims.

Another scheme involves tampering with legitimate bank-owned and -operated ATMs by installing a thin, phony keypad over the real keypad. This phony keypad records PINs and enables identity thieves to obtain sensitive, personal information without ever having to get at the inner workings of the ATM. The thieves just go back and retrieve their phony keypad whenever they think they have captured enough victims, and then download the information. Then they are off to the races.

A third way that people have their identities stolen at ATMs is through the use of small hidden cameras that look over the shoulders of customers inputting their PINs. The cameras record the PINs, and the identity thieves watch the whole transaction without having to be anywhere near the ATM.

What Can You Do to Protect Yourself from Identity Theft at the ATM?

Automatic teller machines are a great convenience, but they also present a significant risk of identity theft. Here are a few tips you should follow to prevent an ATM from turning into an identity thief's jackpot paying slot machine:

1. Avoid privately owned ATMs. Whenever possible, use ATM machines of your own bank. This not only saves you from an increased danger of identity thievery, but also lowers the fees you would otherwise pay for merely accessing your own bank account.

2. Take a careful look at any ATM you are using for indications that its exterior has been tampered with.
3. Look around for hidden cameras. Banks themselves will have cameras, but they are generally embedded in the ATM itself.

The Race to Catch an ATM Identity Thief

Due to the daily limits on the maximum amount of money that you can take out of your bank account through an ATM, large-scale rings of identity thieves have to spend a significant amount of time feeding their phony cards, which carry the stolen information, into legitimate ATMs. One New York City ring was busted in 2001 following the complaints of customers who had noticed that their accounts had been raided. Armed with the numbers of the hijacked accounts and a software program that could locate the specific ATM at which a card was being used, law enforcement was ready for the chase. And a chase it was. Rushing to locations in a crowded city like New York City is no simple task. At times, Secret Service agents stuck in traffic literally had to jump out of their cars and run to the ATM locations in order to try to arrive in time to catch their quarry red-handed. But just as con man Professor Harold Hill said early in the play *The Music Man,* you have to know the territory. And these identity thieves knew the territory. They changed their method of operation to make their ATM withdrawals during the busiest times of the day when both the New York City streets and the sidewalks would be the most congested. And rather than taking the time to use card after compromised card at individual ATMs, the identity thieves kept on the move, using fewer cards at as many as 500 ATM machines. To counter the latest chess moves by the identity thieves, law enforcement began to stake out ATMs that had been the sites of previous fraudulent withdrawals. Then a break finally came. On November 15, 2001, a Citibank employee using ATM withdrawal software noticed that $7,000 had just been withdrawn from a number of different accounts in quick succession at the same ATM. The Secret Service was promptly notified and rushed to the ATM. After a short chase, an arrest was made and the ring was broken.

Mailboxes and Identity Theft

Most mailboxes come equipped with small red flags that when raised indicate that the owner of the mailbox has outgoing mail to be picked up by the mailman. They also can serve as an invitation to identity thieves to raid your mail. An old-fashioned, but still viable, form of stolen mail identity theft occurs when your mail, containing checks to creditors such as credit card companies or your mortgage payment, is grabbed by an identity thief. The thief performs a process known as "check washing" through which the amount of the check and the name of the payee is changed from the person or business to which you made out the check to the name of the identity thief. Common household cleaning products such as bleach can be used to "wash" the check and remove the name of the payee. The check is then rewritten payable to the identity thief in an amount of the thief's choosing.

It is not just your outgoing mail that is fodder for identity thieves. Mail left in your mailbox by the mailman can include new credit cards, Social Security checks, income tax refunds, credit card applications, and credit card statements, as well as other documents that can be utilized for identity theft purposes.

In Oregon in 2012, an identity thief stole checks from the back of a new checkbook that had been sent by mail to the account holder and delivered to the account holder's mailbox where the thief managed to steal the checks. He then merely forged the account holder's name on to the real checks to draw money from the victim's account. Fortunately, the identity thief was at the bank cashing one of the stolen checks at the same time that the account holder was reporting the theft and the identity thief was captured.

Not even legitimate United States Postal Service mailboxes are safe from identity thieves. In April 2004, law enforcement investigators uncovered an identity theft ring in Indiana that utilized a combination of high-technology computers with a low-technology metal device that the identity thieves installed in the familiar United States Postal Service blue mailboxes found on many street corners and into which we all deposit our mail. The device that resembles a snorkel is called a "mail stop." It

collects the mail that later is gathered by the mail thieves without their having to make an apparent break-in to the mailbox, which would have alerted postal authorities. What the thieves looked for was the usual sensitive material, checks and billing account information that could be transformed through sophisticated computer programs to produce phony driver's licenses and blank checks.

TIP

When mailing checks, mail them directly from the post office. Or better yet, try secure online bill paying. As for incoming mail, you might consider a locked mailbox or a post office box at the post office.

TIP

If a credit card bill or bank statement is late in arriving, it might mean that your identity has been stolen and the identity thief has changed the address of the account. Always be vigilant in keeping track of the timely receipt of all financial account documents and bills.

TIP

When ordering new checks, don't have them mailed to your home, where an identity thief can steal them from your mailbox. Pick them up yourself at your bank.

More Mail Scams

In 2012, the postmaster of Newton, Kansas, warned customers of a scam involving people receiving e-mails purported to be from the Postal Service telling customers that a package is being held for them at the post office and that they are being charged a fee for every day that the item has not been retrieved. The e-mail also contains a link for the customer to click on for further information. Unfortunately, if you click on the

link, you will download keystroke-logging malware that will steal your personal information from your computer.

TIP

Never click on any link from a source you are not totally convinced is legitimate. In this case, the United States Postal Services does not send e-mails for unclaimed packages. In any event, if you have any concerns about the legitimacy of such an e-mail, telephone the entity at a phone number that you know is accurate to determine whether the e-mail is a scam.

Identity Theft Threats on the Road

Both business and vacation travelers regularly use their smartphones and other personal electronic devices in airports, at hotels, in coffee shops, and at other public venues where unsecured wireless networks (Wi-Fi) can pose a threat if you do not have proper security software or devices. Also your smartphone security could be breached by an identity thief using Bluetooth. When in public, if you are not using your Bluetooth, turn it off.

TIP

When you are on the road, it is a good idea to encrypt sensitive information and not to input passwords or credit card numbers when using unsecured Wi-Fi. Also, when on the road, be wary of using fax and copy machines to send or copy documents with personal information because these machines might store the information in a fashion available to identity thieves.

Also, the FBI has warned the public about travelers connecting to the Internet in their hotel rooms having their computers infected with keystroke-logging malware when a pop-up appears notifying them of the necessity of updating commonly used software products.

TIP

Make sure that your laptop has been updated with all necessary software changes before you go on vacation. If you are prompted on vacation to update your software through a hotel Internet connection, do not click on the links provided through the pop-up, but rather go directly to the particular software vendor's official Web site to see whether you need to update and do it directly from the vendor's safe Web site.

Another common scam encountered by travelers is a telephone call to your room late at night from someone saying that he or she is the hotel desk clerk and that there is a problem with your credit card and that they need you to provide the number again to them over the phone.

TIP

Again, never give personal information of any kind to anyone whom you have not called and of whose identity you are not absolutely sure. If you receive such a call at your hotel, it is most likely from an identity thief. If you have any question, tell them that you will come down to the front desk in the morning, or you can call the real front desk and see whether an issue does exist.

Identity thieves are also finding hungry travelers a good target. Often identity thieves will put false advertising fliers for restaurant delivery services under hotel-room doors. When the unsuspecting travelers call the telephone number to order, they are asked for their credit card number, which, too often they give, not realizing that they have been scammed until no food arrives.

TIP

Confirm any food fliers with the hotel desk clerk to make sure you do not become a hungry victim of identity theft.

Identity Theft When Giving to Charities

It has often been said that no good deed goes unpunished, and certainly giving to charities is an example of where your good intentions can result in identity theft. Of course, there is always the risk that you are giving to a phony charity. A good place to check out whether a charity is legitimate is the Web site www.charitynavigator.org, which not only will tell you whether a charity is phony, but also will inform you as to how much of the charity's funds go toward its charitable purpose and how much toward administrative costs and salaries.

However, there is another place where even if you give to a legitimate charity, you could be at risk. Most charities are required to file a federal tax Form 990 (Return of Organization Exempt from Income Tax). This form provides much information about the particular charity. A five-year study by the group Identity Finder in 2012 found that almost 20% of all nonprofits required to file Form 990s included the Social Security numbers of charitable donors, scholarship recipients, tax preparers, employees, and trustees on these forms, which are totally available to anyone in the public. The worst part of this is that the law does not even require the inclusion of Social Security numbers on Form 990s. In response to this study, the IRS issued a warning to charities not to include Social Security numbers on Form 990s.

TIP

When making a charitable gift, never disclose your Social Security number to the charity. They don't need it and you don't need them to have it.

TIP

If you are a scholarship recipient, make sure that the organization providing the scholarship does not publish your Social Security number.

Job Scams

Many people search online for jobs through a number of legitimate Web sites including Monster.com. Unfortunately, although Monster.com and many other companies try to monitor their job postings for legitimacy, they do not and cannot guarantee that scammers and identity thieves will not be there.

TIP

Never include your Social Security number or too much identifying personal information on your resume. Often identity thieves will request personal information for a routine background check. Never provide such information until you have checked out the company to make sure that it is legitimate and that the person contacting you allegedly representing the company is legitimate. Identity thieves might ask for your bank account number in order to make a direct deposit of your salary. Don't give this information or any other personal information to a potential employer until you have confirmed not only that the company itself is legitimate, but also that you are not dealing with an identity thief who says he is with a legitimate company. A quick call to the legitimate company's HR department can provide the information you need to make a good decision.

Danger Where You Never Would Expect It

Most copy machines are complex pieces of machinery that since 2002 have contained hard drives that permit scanning, storing of documents, and other high-technology functions. Unfortunately, when you make a copy on such a machine, whatever you have copied remains on the hard drive, so if you were to copy an income tax return on a public copy machine, your personal information would be stored on the computer's hard drive, available to enterprising identity thieves who buy used copy machines. When the Federal Trade Commission became aware of this problem, it notified copy machine manufacturers, and since 2007 all copy machines have been equipped with technology that either encrypts the data on the hard drive or provides for its erasure. Unfortunately, for

copy machines manufactured between 2002 and 2007, this problem still exists.

TIP

Check the date of any copy machine you might use, and if it predates 2007, do not use it for copying documents with personal information that can make you a victim of identity theft. The easiest way to check on the date of the copy machine is to look at the instruction manual.

More Tips for Making Yourself Safer from Identity Theft

The bad news is that you can't do anything to guarantee that you will not become the victim of identity theft. The good news is that there are a number of simple (and not so simple) steps you can take that can reduce your chances of becoming an identity theft victim. Some seem a bit excessive, and perhaps they are, but the decision is up to you. Remember, even paranoids have enemies.

1. Consider paying bills online. It can be cheaper and more secure. But be sure that the online service you are using has security protection. Anytime you provide personal information online, make sure that the site is secure. On Internet Explorer, look for the little lock symbol which shows that your information is being encrypted.
2. Check your bank statements, telephone statements, credit card statements, and brokerage account statements for unauthorized charges. Each month when you get your statements, scrutinize them carefully to make sure that every charge is legitimate. Keep your statements in a safe and secure place. Shred the statements when you no longer need them. If a monthly bill does not arrive on time, promptly notify the company. Sometimes a thief will use your personal information to get your credit card company or other company with which you do business to send your bill to a new address. In this way, the identity thief is able to prolong

the period that he or she is able to fraudulently use your account before you or the company becomes aware of its improper use.

3. Your mother was right. Don't talk to strangers. Updating Mom's advice, don't talk to strangers online. Do not download files that are sent to you from people you do not know. Not only could your computer be damaged through a virus, but you also could be subjected to computer programs commonly called "spyware" that permit an identity thief to access your personal information.
4. Do not carry your Social Security card in your wallet.
5. Get a shredder to destroy all your unnecessary financial records as well as preapproved credit card offers. Dumpster-diving identity thieves can go through your trash to find the mother lode of information for identity theft.
6. Do not write down your PIN or passwords. However, be sure that whatever PIN or password you choose is not something that is easily associated with you, such as your name or your pet's name.
7. Do not store your personal information on your laptop computer. Laptop computers present a tantalizing target for thieves. Many people prepare their income tax returns on their computers, forgetting about the sensitive personal financial information that might be left on their hard drives. Always remove this information from your computer upon completion of your tax return.
8. Get a good antivirus software program and keep it constantly updated. Viruses can infect your computer with spyware programs that, unbeknown to you, might cause your computer to send information stored on your computer to the hacker that can facilitate identity theft.
9. Set up a firewall on your computer. A firewall is a computer program that makes it more difficult for hackers to get access to your computer by preventing or selectively blocking access to your computer through the Internet There are many good firewall programs that are easy to install on your computer.
10. When you get rid of your computer, it is not enough to merely delete personal information. Deleted information remains on

your hard drive and can be readily accessed by a computer-savvy identity thief. Make sure you use one of the special programs, such as the free program Eraser, that will effectively remove the information from your hard drive. Alternatively, you can do what I prefer to do, which is remove the hard disk from the computer and smash it into oblivion with a hammer.

11. Take advantage of obtaining your annual free credit report from each of the three credit-reporting agencies—Equifax, Experian, and TransUnion—so you can look for unauthorized charges and evidence of identity theft, as well as make sure there are no innocent mistakes on your reports that could harm your credit. Obtain your free credit reports on a staggered basis from each of the three credit-reporting agencies and get one every four months for better, more current protection. You can get your report from Equifax at www.equifax.com, from Experian at www.experian.com, and from TransUnion at www.transunion.com.

12. Put a credit freeze on your credit report at each of the three credit-reporting agencies. Through a credit freeze, you are able to prevent access by anyone to your credit report even if they have your Social Security number. You are the only one who has access to your credit report, by way of a PIN that you pick. If you need to apply for credit, you can temporarily lift the freeze on your credit report and then put it back when the company you want to have access to your report has finished.

13. If you are in the military and deployed away from home, you can place an active duty alert on your credit reports at each of the three credit-reporting agencies that lasts for a year and can be renewed if necessary. This will restrict access to credit without your approval.

This page intentionally left blank

3

Danger on the Computer and What to Do If You Are the Victim of Identity Theft

Sometimes it is hard to remember what life was like without personal computers, smartphones, and iPads. Imagine life without Angry Birds. E-mail, shopping online, and surfing the Net are only three of the uses of personal computers that are taken for granted in our everyday lives. But as much as computers have enriched our lives, they have also made us much more vulnerable to identity theft. The first step in reducing your vulnerability to identity theft through your computer is learning where you are vulnerable. However, assessing your risk is not enough. Unfortunately, there is nothing you can do to guarantee that you will not become a victim of identity theft, so it is also important to know what to do if you become an identity theft victim.

Spyware

The Good: The *I Spy* television series that ran from 1965 to 1968 and starred Bill Cosby and Robert Culp.

The Bad: The *I Spy* movie released in 2002 starring Eddie Murphy and Owen Wilson.

The Ugly: Spyware, computer software that can be used to gather and remove confidential information from your computer without your knowledge.

Everything you do online, including your passwords, might be vulnerable to spyware. Spyware can put you in great danger of becoming a victim of identity theft. To make the problem even worse, some forms of spyware can be installed on your computer from a remote location without the identity thief ever having physical access to your

computer. You would think that it would be difficult for the ordinary person to find spyware, but it is not. Typically it is used by employers monitoring employees' computer use and parents who monitor their children's computer use. It has been rumored that sometimes it is even used by a not-too-trusting spouse who wants to know what his or her spouse is doing online. In addition, some file-sharing programs also contain spyware. Sometimes this information is used merely to send you advertisements for products and services that might interest you. "Cookies" planted by the spyware can be used to monitor your Internet use. Although cookies invade your privacy, they might have no more insidious intention than to tailor advertising to your specific interests. Although spyware does invade your privacy, you might have actually agreed to have spyware installed on your computer when you went to a particular Web site and accepted that Web site's user agreement, which can be long and filled with fine print that hardly anyone reads. Unfortunately, identity thieves looking to steal your identity and maybe your money also use spyware.

What Can You Do About Spyware?

Sir Isaac Newton's Third Law of Motion was that for every action, there is an equal and opposite reaction. This also seems to apply to modern computer use (or misuse). For every spyware program, there also are antispyware programs that can let you know if your computer has been infected by spyware. Interestingly enough, some spyware developers use antispyware software to test the effectiveness of their own spyware and to try to make it less vulnerable to detection.

Although remote installation of spyware occurs, many spyware programs must be physically installed on your computer, so it is important to be sure you trust whoever repairs and services your computers.

Another way to protect yourself is through the installation of software programs that record every software installation that occurs on your computer. If you use this software, you obviously want to keep it hidden so that someone attempting to install spyware on your computer would be unaware that they are actually being monitored.

Some antivirus programs also work against spyware and they provide good additional, if not total, protection.

You can also take advantage of your Web browser's ability to prevent or limit cookies by changing your preference to disable cookies. An easy place to go to learn how to disable cookies is http://privacy.getnetwise.org/browsing/tools/.

Finally, return to Sir Isaac Newton and add to his laws of motion the axiom "If you can't beat them, join them." Because spyware permits all your computer's activities to be recorded, one way of telling that your computer has been accessed by someone with spyware is to install your own spyware in order to determine what has been going on in your computer.

It's Not Always Good to Share

File sharing is a way for people to share music, computer software, or games over the Internet. It is simple to do. You just download software that permits you to connect your computer to a network of other computers using the same software, and you are off to the races. Unfortunately, there are some significant risks involved in file sharing. If you do not install the file-sharing software properly, you might make your computer vulnerable to having personal information stored on your computer retrieved by an identity thief through spyware.

Botnets

A botnet is a web of infected computers used by identity thieves and scam artists (the only criminals we refer to as artists) to send out spam, viruses, and malware. Unwittingly, you might even be part of the problem. It has been estimated that as much as 20% of home computers have been compromised by botnets that occur when, unwittingly, people download the malware and become part of the botnet. Often the malware is downloaded through clicking on a link from an e-mail or phishing Web site promising free music, games, or other enticements.

TIP

Often people find out that they are part of a botnet when their friends start receiving spam or malware-infected e-mails from the e-mail address of the person whose computer has been taken over as a part of the botnet. If that happens to you, you should do a full security scan of your computer and remove or quarantine the offending virus. Then you should change your password to a better, more complex password.

In 2011, the Department of Justice with the assistance of Microsoft Corp. disabled a massive botnet that infected as many as two million computers for as long as ten years. This particular botnet originated in Russia and has been estimated as having led to the theft of $100 million over the ten years the botnet was in existence.

Celebrity Malware

Identity thieves are quite current in pop culture and are always ready to take advantage of the public's curiosity to lure us into downloading malware such as keystroke-logging malware onto our computers. Celebrity deaths, in particular, have provided a rich vein of identity thefts when people receive e-mails or postings on their Facebook accounts purporting to provide new and sometimes salacious details regarding the deaths of celebrities, such as Michael Jackson, Amy Winehouse, Steve Jobs, and Whitney Houston.

TIP

Always consider the source, and remember, you can't trust an e-mail from a "friend" that promises to link you to a story about something that intrigues you, because you cannot be confident that the e-mail is from your "friend." His or her e-mail might have been hacked. And even if the link is from one of your real friends, he or she might be merely passing on a corrupted link that can victimize both of you. Get your online information only from reliable sources.

Help You Just Don't Need

According to a survey by Google, 15% of malware can be traced back to phony pop-ups that tell you that your computer has been infected by a virus and that you need to download their software to remedy the problem by linking to their antivirus software. Sometimes these phony pop-ups just steal your money and provide you with no solution to a problem that you do not have. Other times they prompt you to provide personal information that is used to make you a victim of identity theft.

TIP

Close your browser if you get this kind of a pop-up, then go to the anti-virus and security software program sites that you use, run a scan of your computer, and make sure that your legitimate security software is up-to-date. It is a good idea to use security software that provides for automatic updating.

Just When You Thought It Was Safe to Go Back to Your Computer

People are always interested in firsts. Charles Lindbergh was the first man to fly solo across the Atlantic Ocean. Neil Armstrong was the first man to set foot on the moon. And 19-year-old Drexel College student Van Dinh was the first person to be charged by the Securities and Exchange Commission with fraud involving both computer hacking and identity theft. I am sure his parents are quite proud.

Dinh's story began in late June of 2003 when he bought 9,120 put option contracts on Cisco stock at a strike price of $15 per share. The cost to Dinh for each option contract was $10 per contract, for a total of $91,200. Each put option gave him the right to sell 100 shares of Cisco stock at $15 per share if the value of the Cisco stock fell to that price or below before the date of the put option contracts, which expired on July 19, 2003. For example, if the stock price fell to $14 per share, Dinh's ability to sell the shares at $15 per share according to the put option

contracts would have resulted in a profit of $912,000. And if the stock fell even further, this highly speculative investment would have paid off even more handsomely. There was only one problem: With nine days to go before the expiration date of his Cisco put option contracts, the stock was trading at $19 per share, which meant that if that price level was maintained, his put option contracts would be worthless at their expiration.

According to the FBI, instead of just taking the potential loss, Dinh concocted an elaborate computer-hacking and identity theft scheme to bail himself out. What Dinh needed were victims upon whom he could unload his soon-to-be-worthless put option contracts. The first step was to find those victims. Dinh did this by going online to the investment analysis Web site StockCharts.com's stock-charting forum. Using the name Stanley Hirsch, Dinh e-mailed a message to at least 50 StockCharts.com members asking whether any of them maintained their own Web sites. When a Massachusetts investor responded to the e-mail, the first step in the fraud had been completed. By replying to Dinh's seemingly innocuous e-mail inquiry, the Massachusetts investor provided Dinh with the investor's personal e-mail address. The next day, Dinh, now using the name Tony T. Riechert, contacted the unwary investor by e-mail and invited him to participate in a beta test of a new stock-charting tool. Beta testing is a common practice in the software development world in which individuals are solicited by companies to try out new versions of computer programs being developed as the companies try to get the "bugs" out of them. Continuing to swallow the bait, the Massachusetts investor accepted the invitation and downloaded the purported stock-charting software through a link in the e-mail message.

Unfortunately, the program was actually just a ruse known in the computer world as a "Trojan horse." A Trojan horse is a computer program containing harmful codes hidden within an apparently harmless program. In this instance, a number of keystroke-logging spyware programs were contained within the Trojan horse. Keystroke-logging spyware programs, as I described earlier, permit an Internet user at one location to monitor all the keystrokes of another unsuspecting Internet user at a different location. Talk about food for paranoids! When the keystroke-logging program known as "The Beast" was lodged in the Massachusetts investor's computer, Dinh simply had to wait and monitor his victim's

computer use. From there, he found the last pieces of critical information necessary for his scam—the victim's password and login information for his online brokerage account with TD Waterhouse.

On July 11, 2003, with only eight days left before the expiration of his Cisco put option contracts, Dinh hacked into his victim's TD Waterhouse account and made a series of Cisco option buy orders using up almost all the available cash in the victim's account. These buy orders were, in turn, executed on the Chicago Board Options Exchange and filled with options sold from Dinh's account, thereby avoiding a significant loss by Dinh. Four days later, the Massachusetts investor, shocked to see that his brokerage account had been raided, notified the Securities and Exchange Commission.

FBI and SEC investigators did not take long to trace the relevant e-mails. The e-mail from Tony Riechert was found to have come from Lockdown Corporation, a company that provides, in the words of the FBI, an "anonymizing" service to its customers that permits the true identity of the original sender of the e-mail to be hidden. Lockdown Corporation cooperated with the investigators and provided information which showed that the initiator of the Tony Riechert e-mail also had gone to the TD Waterhouse Web site and a hacker Web site that provided access to keystroke-logging spyware programs. The noose was tightening. Further investigation led to an Australian Internet service provider, as well as e-mail servers in Ireland and Germany. Ultimately, the electronic trail led to Van Dinh, who cooperated with investigators and provided SEC attorneys with information and documentation connecting him to the crimes.

The Lesson

The lesson could be the old one that crime does not pay. In Van Dinh's case, he was promptly caught; plus, his scheme only served, at best, to reduce the extent of his losses. However, for the rest of us, the lesson is first to be aware that Trojan horses and keystroke-logging spyware programs exist. These invasions of your personal information cannot harm you unless you invite them in. Keep your virus software constantly updated. It is a good practice to be wary of downloadable programs offered from e-mail, forums, or advertisements if you are not absolutely positive that they are legitimate. The lesson for brokerage houses is

to maintain better security. Software is available that is able to detect changes in patterns of account holders or a sudden, large liquidation of funds. The Patriot Act, enacted in the wake of the attacks of September 11, 2001, also serves to help investors by requiring cross-referencing of personal information by financial service providers.

Wi-Fi: A Convenience to Worry About

Advances in computer technology are great. Unfortunately, they also often bring with them opportunities for identity theft. Starbucks is a very successful company. One of the perks of being a Starbucks customer is that they provide wireless Internet access in their stores so people can sit back, drink some expensive coffee, and search the Internet. The way wireless Internet service, or Wi-Fi, works is by sending Web pages over radio waves to computers that have wireless capabilities. It is easy for technologically sophisticated identity thieves to hack into the computers of customers who are using their laptops at wireless access points, often referred to as Internet "hotspots." Savvy hackers can join the network and access the information contained within the computers of users of the system. Wi-Fi is found more and more at malls, bookstores, and even McDonald's restaurants. Securing your laptop computer from hackers while using Wi-Fi facilities is complex and particularly difficult for the relatively unsophisticated technology user who often is also unlikely to keep his or her computer security and virus protections up-to-date.

TIP

Any computer that has wireless capabilities activated should also have security software installed at the same time. One of the best ways to protect yourself when using Wi-Fi is to encrypt your data. Make sure your wireless router has an encryption mechanism and that it is turned on. Even wireless routers that have encryption capabilities are often delivered with this feature turned off. It is up to you to make sure that your encryption feature is functioning. Most wireless routers also have a feature called identifier broadcaster that announces your presence to other

devices within the Wi-Fi area. Make sure that yours is turned off so you are not alerting anyone to your computer's presence. Finally, even if your identifier broadcaster is turned off, wireless routers come equipped with a standard default identifier for your particular computer. This default identifier is known by identity thieves and hackers, so change your identifier so that your computer cannot be accessed by identity thieves and hackers. And while you are at it, change your wireless router's default password to your own, more complex password.

E-Mail Dangers

Checking our e-mail the first thing in the morning for many of us is as common as a morning cup of coffee. In fact, although most people will only have, at most, a couple of cups of coffee throughout the day, most of us check our e-mail constantly. It is a way of life.

Unfortunately, too many of us are careless when it comes to protecting our security when using e-mail, thereby making us vulnerable to identity theft. Sometimes the problem is the use of passwords that are too easy to guess.

Inadequate passwords present a danger not just on your e-mail account, but on any account that you use that requires a password. Following a hacking incident involving the company RockYou.com, which makes software for use on social networking sites, a list of 32 million passwords became public and confirmed what many of us already thought was the case—that too many of us use passwords that are far too easy for an identity thief to guess. The most popular password is the far from difficult to guess "123456" followed closely by the almost as difficult to guess "12345." Other common and much too easy to guess passwords include "password," "letmein," "trustno1," "iloveyou," and the seemingly difficult password "qwerty," which might appear to be a complex password until you look at the top row of letters on your computer keyboard.

Identity thieves and hackers can use computer programs to guess at huge numbers of passwords, and yours might just be too easy to guess.

TIP

As difficult as it might seem to remember, a password that is at least 12 characters long and contains a mix of letters and symbols will provide you with greater security. Having the letters and symbols relate to an easily remembered sentence is an effective way to come up with a secure password. "4score&7yearsago@my house" is a good example.

Another source of problems with e-mail security is a security question that is too easy for an identity thief to guess. Security questions are helpful in protecting your e-mail from being hacked by an identity thief, but if the question is too easy to guess, you might have unwittingly handed the key to your e-mail account to an identity thief. Unfortunately, too many people put too much information about themselves online through social media, such as Facebook. This makes it easy for enterprising identity thieves to get access to your e-mail account by logging on to the account, and then indicating that they have forgotten the password or want to change the password. In both instances, a security question is used by the e-mail provider to confirm that the person is the legitimate user of the account. David Kernell was convicted of stealing access to former Alaska Governor and Vice Presidential candidate Sarah Palin's e-mail merely by answering her security question, which was where did she meet her husband. A quick trip to Wikipedia provided the answer to the question, which was Wasilla High School, and it was a simple matter from there for Kernell to change her password and take over her account.

Bad Apples

For many years, Apple computer users were confident that most computer viruses were directed at users of PCs rather than Macs. For a while that was true, mainly because there were just more PC users than Mac users, so it was more worth the time of identity thieves and scammers to target PC users. But all that has changed with the increased popularity of Apple computers, so now Mac users must be every bit as vigilant as PC users when it comes to protecting their computer security.

Typos Can Be Dangerous

Typographical errors are common, but they also can be dangerous. This is because identity thieves have registered the domain names of common misspellings of popular Web sites, such as Walmart or Apple, in an effort to lure you to their own Web sites. These sites look like the Web sites of the legitimate companies you are seeking, but unfortunately they trick you into providing personal information that can be used to make you a victim of identity theft or prompt you into downloading dangerous keystroke-logging malware that can steal your personal information from your computer.

Stories

Unfortunately it is not enough to do all that you can to protect the data that, in the hands (or computer) of an identity thief, can lead to trouble for you because you are only as safe as the weakest security programs of the companies and agencies with which you do business.

A Towering Problem

It is important to be sure that any company with which you do business protects your personal information; however, sometimes the assurances of those companies mean little. The FTC recently brought a complaint against Tower Records. The company claimed that it used state-of-the-art technology to safeguard the personal information of customers. However, the security system it used permitted online users of its Web site to access personal information about other Tower customers. According to the FTC, this flaw in the security system was easy to fix, but Tower failed to do so until it was compelled by a formal complaint of the FTC that was settled in April 2004. In this case, as with all FTC settlements, Tower did not admit that it did anything wrong yet agreed not to do it again.

We Regret to Inform You

In March 2004, GMAC notified 200,000 of its customers that their personal information might have been compromised (a euphemism for "possibly stolen") following the theft of two laptop computers used by

GMAC employees that were stolen from an employee's car. Although the data stored on the particular laptop computers was protected by password-access technology, the data itself was not encrypted as a further prudent security measure. The data itself was extremely sensitive material, including names, addresses, birth dates, and Social Security numbers of GMAC customers. This security breach is not uncommon in an era when employees may take work home on their laptops.

It is not even just the companies with which you do business that should concern you. It is also the companies with which they do business and with which they might share your personal information. In 2003, the Bank of Rhode Island contacted 43,000 of its customers to warn them that their personal information, including Social Security numbers, might have been compromised. A laptop computer used by an employee of Fiserv, Inc., a company with which the Bank of Rhode Island did business, was stolen. This laptop computer contained sensitive personal information about Bank of Rhode Island customers.

California, a state that has often been the leader in identity protection laws, has had a law since 2003 that requires any business that has had a breach of its computer security to notify its customers. Similar laws are expected to be passed in other states, although it would be even better if companies paid greater attention to preventing their systems from being improperly accessed in the first place.

Keys to Identity Theft

It was bad enough that two Wells Fargo employees left the car keys in the ignition of their unlocked rental car during a stop at a Missouri gas station convenience store while they went inside in February 2004. When they came out, their Ford Mustang was gone. But also gone with the car was the laptop computer that they had left unattended in the trunk of the car. The computer contained the names, addresses, and Social Security numbers of thousands of Wells Fargo mortgage customers. The car was retrieved less than a week later, but the computer was gone. A password was required to access the personal information stored on the computer, but the simplicity of that task to a computer-savvy identity thief left Wells Fargo's mortgage customers in substantial danger of identity theft.

TIP

Ask any company with which you do business about their policy for the security and protection of personal information, including whether your information is encrypted in their computers. If their answers do not satisfy you, take your business elsewhere.

If You Can't Trust Your Lawyer, Whom Can You Trust?

If you can't trust your own lawyer, whom *can* you trust? My grandmother, the same one who used to say that she could keep secrets but that the people to whom she told them could not, used to refer to me as her grandson "the liar." I used to try to correct her, telling her that the name of my profession was pronounced "lawyer," to which she always responded, "Don't correct me, I know what I'm saying." I think my grandmother was kidding. I hope my grandmother was kidding, but many people do consider lawyers just a bunch of liars. The case of Iric Vonn Spears, unfortunately, does little to dispel that impression. Iric Vonn Spears was an attorney who, having access to the personal information of his client Reginald Dalton, used that information to steal Dalton's identity and buy a home and open credit card accounts. The house of cards tumbled when the real Dalton was contacted by the bank that held the mortgage on the home purchased by Iric Vonn Spears using the name of Reginald Dalton, telling him that the mortgage was being foreclosed. Iric Vonn Spears was convicted of grand theft, mortgage fraud, identity fraud, and forgery. He was sentenced to ten years in prison.

Lures

Prior to the release in late 2012 of the *Halo 4* Xbox video game, some identity thieves were circulating e-mails and Web sites promising free copies of the game before its official release. These were just phishing scams intended to lure gamers into downloading keystroke-logging malware that would lead to identity theft. Similar scams occur prior to the release of other new video games and the latest versions of technological devices.

You Can Bank on This Being a Scam

The FBI has warned people about a phishing e-mail purportedly from the National Automated Clearing House Association (NACHA), the Federal Reserve Bank, or the Federal Deposit Insurance Corporation telling you that there are problems with your bank account and that you need to click on a link for further information and to fix the problem. Those people who click on the link download keystroke-logging malware.

TIP

If you get such an e-mail, immediately delete it. None of these agencies will contact you by e-mail. If you have any concerns, contact your bank by phone at a telephone number that you know is correct.

A Few Ounces of Protection—Protecting Yourself Online from Identity Theft

Merely because you are vulnerable to identity theft on your computer is no reason to avoid using your computer to access the Internet; however, some good protective measures can go a long way toward protecting yourself while you are online:

1. Install good security software to protect your computer from viruses, spyware, and other malware. There are many legitimate companies that offer free security software, but make sure that you are dealing with a reputable company and consider paying for a product that will provide you with greater protection.
2. Keep your security software up-to-date. Automatic updates are best.
3. Encrypt the data on your laptop. Microsoft's BitLocker will do the job free; however, it is available only with Windows 7. TrueCrypt is another free encryption service that will protect the data on your computer from prying eyes in public.
4. Use strong, difficult-to-guess passwords.

5. Never turn off your firewall. Firewalls maintain a protective barrier between your computer and the Internet.

6. The price of computer security is eternal vigilance along with a healthy dose of mistrust. Never download anything from a source that you do not absolutely trust, and even if you trust the source—don't. First communicate with the source to make sure that the material you are being asked to download or link to is actually from that person or company that you trust, and even then, remember that they could have been compromised and could be unintentionally sending you corrupted material.

7. Regularly get, and review for accuracy and signs of identity theft, a copy of your credit report. You are entitled by law to get a free copy of your credit report annually from each of the three major credit-reporting bureaus, Equifax, Experian, and TransUnion. The most efficient way to do this is to request a copy in sequence from one of them every four months. This way you stay more current in your review of your credit report, at no cost. It is also important to remember that there are a number of services that will lead you to think that you are ordering a free credit report from them, but in the fine print you will find that you have signed up for a continuing costly service that you might not need or want. The only place to get your truly free credit report is www.annualcreditreport.com or by phone at 877-322-8228.

8. If you are in the military and are deployed overseas, you can request that an active duty alert be put on your credit report that will not permit credit to be issued without your specific approval for a year. The active duty alert can be extended after the first year for additional years. You can also designate a personal representative here in the states to give approval on your behalf if you are applying for credit while overseas but can't be reached.

A Pound of Cure—What to Do If You Are a Victim of Identity Theft

Don't feel too bad if, despite your best efforts, you become a victim of identity theft. You are in good company. The list of prominent victims

of identity theft includes Oprah Winfrey, Michael Jordan, Tiger Woods, Steven Spielberg, Ted Turner, Warren Buffet, New York City Mayor Michael Bloomberg, Robert DeNiro, Martha Stewart, Will Smith, and Ross Perot. Fortunately, there are some steps you can take to respond to the theft of your identity and to minimize the damage:

1. Put a fraud alert on your credit report. If you think that you might be the victim of identity theft, you can have a fraud alert placed on your credit report at the credit-reporting agencies. The alert stays on your report for up to 90 days but can be extended for up to seven years. When a fraud alert has been put on your credit report, you are entitled to a second free credit report during that year in order to monitor your credit for further irregularities. In the past, people placing a fraud alert on their credit reports found that for it to be effective, they had to call each of the three major credit-reporting agencies to have fraud alerts independently placed on each company's record. Now, under FACTA (the federal Fair and Accurate Credit Transactions Act), all you need to do is call one of the credit-reporting agencies and they are required to notify the other two to place the fraud alert on your file. Unfortunately, fraud alerts are not always as effective as you might think. The law does not require businesses to check for fraud alerts before granting credit, and there are no penalties for companies failing to monitor credit reports for fraud alerts. Many companies do not even bother to check for fraud alerts, and due to technical procedural problems, notifying one of the credit-reporting agencies to place a fraud alert might not result in a fraud alert being placed on your credit report at the other two credit-reporting agencies.
2. A better solution might be to place a credit freeze on your credit report. This service, available in all states, permits you to effectively seal your credit report from access by anyone (such as an identity thief with your Social Security number and other personal information) without the use of a PIN that you pick to make your credit report available. Thus, an identity thief is prevented from using your credit report to secure credit or open a new account in your name. Consumers Union has a very

user-friendly Web site that can help you access the credit-freeze law for your particular state by going to www.consumersunion.org/campaigns/learn_more/003484indiv.html#MA. Even if you have not been a victim of identity theft, a credit freeze is a great preventive measure to take to protect yourself from identity theft.

3. Go to the Federal Trade Commission Web site or to Chapter 21, "Form Letters," to obtain the FTC's ID Theft Affidavit, and use it to report the crime.

4. Contact all your creditors by phone and then follow up with a letter sent by certified mail, return receipt requested. See Chapter 21 for a sample. Get new credit cards with new account numbers. Change your PIN and your passwords.

5. Close tainted accounts. When opening new accounts with these creditors, use a password that is not easily connected with you. A word to the wise: Do not use your mother's maiden name, or to be particularly safe, do not even use my mother's maiden name. People think that their mother's maiden name is difficult to find. It is not. It is on your birth certificate, a public record.

6. When you close accounts, make sure that the accounts are designated as being closed at the customer's request due to theft so that when information is transmitted to the credit-reporting bureaus, it is clear that the problems are not of your doing.

7. Ask your creditors to notify each of the credit-reporting agencies to remove erroneous and fraudulent information from your file.

8. If your checks are stolen, promptly notify your bank and have the account closed immediately. If your checking account is accessed by checks with forged signatures, you obviously have not authorized the withdrawals and should not be held responsible for money stolen from your account. However, if you neglect to monitor your account and fail to promptly notify your bank when there is an irregularity in your account or your checks are lost or stolen, you might be held partially responsible for your losses. It is not even necessary to have your checks physically

stolen for you to become a victim. An identity thief armed with your name, checking account number, and bank routing information can use one of a number of inexpensive computer software programs to create checks for your account.

9. Contact the various check-verification companies and ask that they, in turn, contact retailers who use their services, telling them not to accept checks from your accounts that have been accessed by identity thieves. Check-verification services are companies that maintain databases of bad check writers. Retailers using their services contact the verification service's database before accepting checks. Among the companies that do check verification are CellCharge, CheckCare, and CrossCheck.

10. To see whether checking accounts have been opened in your name, contact ChexSystems at www.consumerdebit.com to request a free copy of a report that lists all checking accounts in your name. If you find that an account has been opened in your name, contact the bank and instruct them to close the account.

11. File a report with the police both where the fraud occurred and where you live. You might find police departments reluctant to accept your report, sometimes for technical legal jurisdictional reasons. Politely insist that they at least accept your report. Remind them that credit bureaus will prevent fraudulent accounts from appearing on your credit report if you can provide a police report. Give the police officer taking the report as much documentation as you have to support your claim, including the ID Theft Affidavit approved by the Federal Trade Commission that appears later in this book. When a police report has been filed, send a copy of it to each of the three major credit-reporting agencies.

12. Be proactive. Contact your creditors where you have tainted accounts and get a written statement from each of them indicating that the account accessed by an identity theft has been closed and that the charges made to the accounts are fraudulent. Request that they initiate a fraud investigation. Find out what you are required to do to advance the investigation, such as

providing them with a police report. A sample letter to your creditor requesting such a statement from your creditors is included in Chapter 21. These letters can be very helpful, particularly if the credit-reporting bureaus mistakenly resubmit the fraudulent charges on your credit report. Remember to get a written copy of your creditor's completed investigation.

13. Send copies of your creditors' completed investigations to each of the three credit-reporting agencies. Ask them to send you a copy of your updated credit report in order to confirm that any erroneous and fraudulent information has been removed from your file.

14. If fraudulent charges do appear on your credit report, notify the credit-reporting bureaus in writing that you dispute the information and request that such information be removed from your file. A sample letter is included in Chapter 21.

15. If you are contacted by a debt collector attempting to collect a debt incurred by an identity thief in your name, write to the debt collector within 30 days of receiving the initial notice from the debt collector. Tell the debt collector that the debt is not yours and that you are a victim of identity theft. Send a copy of the identity theft report, police report, or other reports you might have completed. After you provide this information, the debt collector is required by law to cease collection efforts until they have verified the accuracy of the debt. Additionally, you should also contact the company for which the debt collector is attempting to collect the debt and explain to them that the debt is not yours, but rather is the result of identity theft. Also, ask them to provide you with details about the transaction creating the debt, including copies of documentation that might contain the signature of the identity thief. Finally, contact the credit-reporting agencies and ask that they block the incorrect information from appearing on your credit report. Details for how to do this can be found in the chapter on credit reports.

16. If your driver's license is possibly in the hands of an identity thief, you should cancel the license and get a new one.

17. If your passport is lost or stolen, contact the State Department at www.travel.state.gov/passport to arrange to get another passport and to have it recorded that your passport has been lost or stolen.

18. If your mail has been stolen and used to make you a victim of identity theft, the Postal Service will investigate the crime. Notify the postal service at your local post office.

19. If an identity thief has used your identity to set up phony accounts for utilities such as phone, cable, electricity, or water, contact the utility provider and report the crime. Provide them with a copy of your identity theft report and close the account. You should also contact your state public utility commissioner's office and inform them about the crime and provide them with your identity theft report so that they can investigate this as well.

20. If your information has been used to obtain a student loan in your name, contact the school or the lender, provide them with the identity theft report, and ask them to close the loan. You should also report the crime to the U.S. Department of Education at www.ed.gov/about/offices/list/oig/hotline.html.

21. If your Social Security number has been misappropriated by an identity thief, contact the Social Security Administration at www.socialsecurity.gov, or by phone on their fraud hotline at 800-269-0271, or by mail at Social Security Administration Fraud Hotline, P.O. Box 17785, Baltimore, MD 21235.

Index

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Y

Z