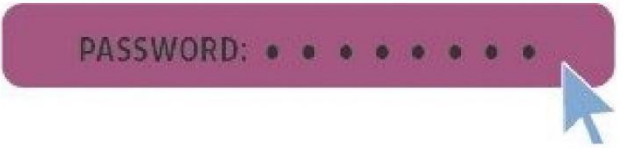
NICK SELBY • HEATHER VESCENT

# THE CYBER ATTACK SURVIVAL MANUAL

TOOLS FOR SURVIVING EVERYTHING FROM IDENTITY THEFT TO THE DIGITAL APOCALYPSE




Illustrations by
ERIC CHOW
and Conor Buckley

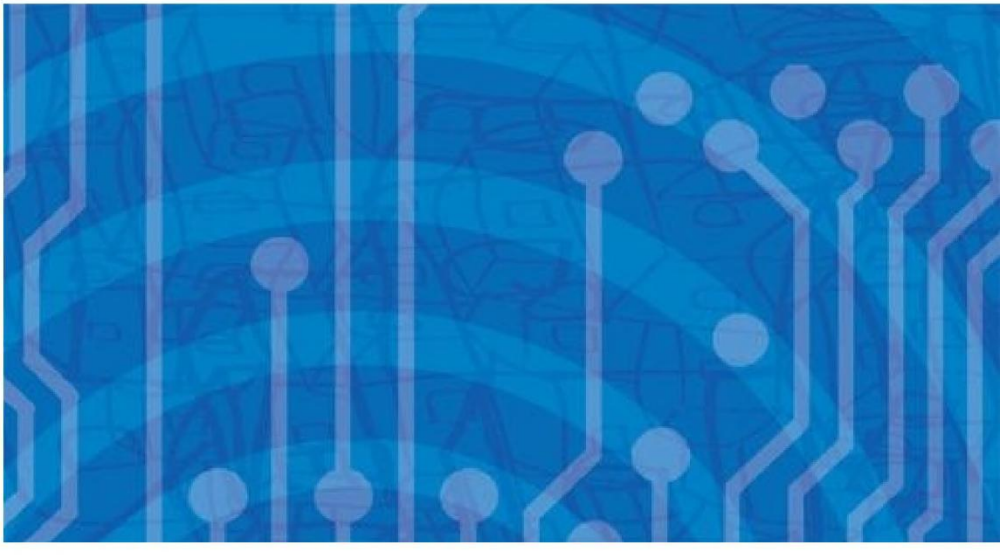
weldonowen

# CONTENTS



# HACK YOUR LIFE





# HACK SOCIETY

# HACK THE WORLD

# THIS BOOK IS ALREADY OUT OF DATE (AND THAT'S OKAY)

Every day there seems to be a new story about cybercrime: millions of credit cards stolen, private celebrity photos leaked, foreign agents interfering at the highest levels of government. It's hard for even the best-informed reader to know how much of this is real versus scare-mongering clickbait, and how to react regardless. Sadly, many people either become so paralyzed by fear that they vacillate between different strategies for too long/ Conversely, some decide it's all too much and try to ignore the topic completely.

The thing is, each of us is utterly reliant on cybersecurity in ways both obvious and unexpected. As a police officer, I've brusquely knocked on the door of the suspect in a cyber case only to find a 78-year-old retiree, innocent of anything but a yen for some specialized, icky, but legal pornography. Our man made a rookie mistake by going for the free icky-but-legal porn, unaware of the first rule of the web: if you can't figure out how someone makes money on a site, you're the product. Criminals had planted malware in his naughty movies and were renting cyber scammers remote access to his computer, unbeknownst to him.

Some of the hacks we describe will be old news tomorrow. Some will take on new and more insidious forms. And something new will pop up every time you turn around. That's okay—this

book gives you the tools you need to understand what your digital footprint looks like to criminals, advertisers, investigators, and governments, and how to figure out and fix your vulnerabilities even as the specific threats change.

We can't tell you everything that might happen to you—some of next week's threats are being cooked up right now in basements and labs from Missouri to Moldova. But we can tell you how to reduce your risks no matter what. Security experts like to talk about OPSEC (operational security). And OPSEC is OPSEC—today and forever. It's not about specific dangers, it's about a mind-set of preparedness.

Understanding your digital universe and the consequences of your actions will reduce the things that can make you a victim, without your having to miss out everything the internet has to offer. This book will help you better understand the kinds of threats out there, and give you the tools and perspective to protect yourself. The rest is up to you.

**NICK SELBY**

## ALSO, THIS BOOK WILL
# FREAK YOU OUT
## (AND THAT'S ALSO OKAY)

To put it simply, you're in danger. Your identity, your bank accounts, your kids, and even your government are vulnerable to attack from cyber criminals around the world. That should freak you out. But this book is much more than a collection scary stories (although it's that too). It's also a toolkit for protecting yourself and your data in an increasingly dangerous online world.

The digital age has given us a dazzling array of products and services at our fingertips, but also created new and often unexpected problems. Security technology will continue to get better—and criminals will keep finding new ways to get around that technology. That's where we come in.

How to get your head around security in the modern age? Most people want to know first and foremost how to avoid getting hacked. That's the wrong mindset. It's almost inevitable that you're going to be hacked at some point in your life online.

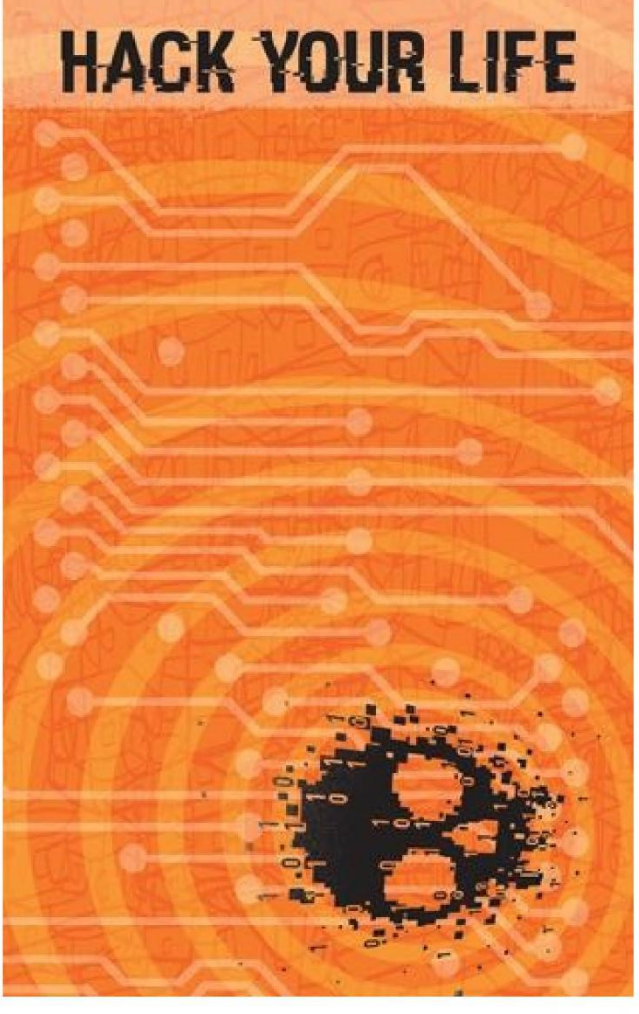
Start with the assumption that even the most secure technologies are vulnerable. There's an ongoing war between criminal hackers and security experts, and that's not going to change. The only way we can "win" is to assume everything will be hacked, and take precautions to secure what is important. If you expect this inevitable hacking of your security systems, you will be able to understand the risk factors and monitor your

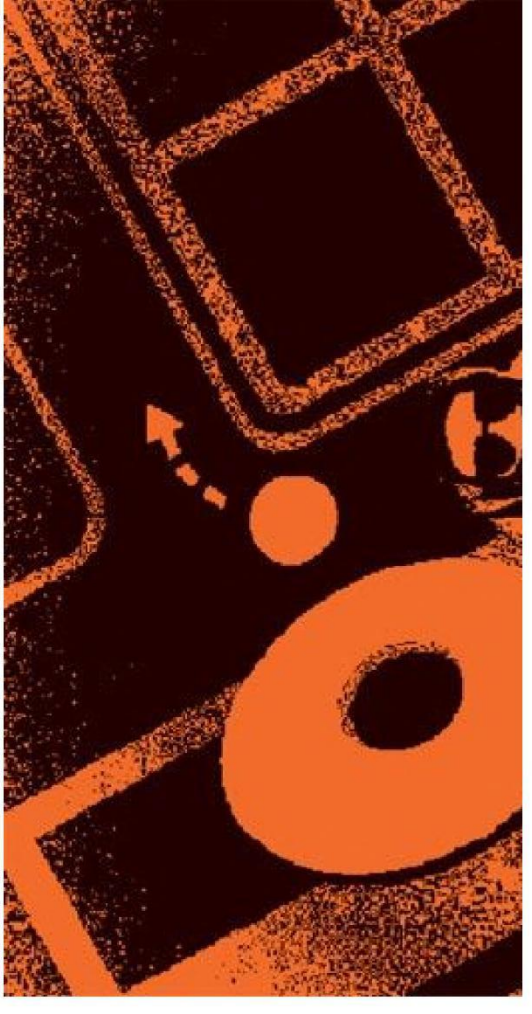
security on an ongoing basis. You'll know the places you are vulnerable and be able to take appropriate precautions.

How to know which are the appropriate precautions? That's easy. Read this book! Many of the vulnerabilities enumerated in this book can be dealt with relatively easily, once you have the know-how. You don't need to have the most secure system, just the best one for your needs. Not sure what those are? We'll help you figure that out.

In a sense, hackers, in their own way. Every time they break a system, we learn something new about its vulnerability, and how to make it more secure. I personally look forward to the new and exciting ways hackers will point out the limitations of each new technology. I just don't want them learning on you!

**HEATHER VESCENT**



Your bank account is suddenly, mysteriously overdrawn. Everyone in your address book gets a desperate email from you asking for money. You fail what should have been a routine background check. Your TV starts getting unusual error messages. What's going on? Cybercrime can, quite literally, hit you where you live—and it's getting more common all the time as our lives get more connected and hackers more sophisticated. The chapters that follow tell you what to do when Internet bad guys make it personal—stealing your identity or your money, invading your privacy, bullying your kids, or even threatening your life. We also highlight some unexpected vulnerabilities in your smart phone, your browsing habits, and your household appliances, as well how to keep your personal information safe and secure.

CHAPTER 1

# KEEP YOUR IDENTITY SAFE

**IDENTITY THIEVES CAN BUY, SELL, OR CAPTURE YOUR IDENTITY AND USE THE INFORMATION TO GET MONEY AND SERVICES`—OR USE YOUR NAME, CREDIT RATING, OR INSURANCE TO TAKE OUT A LOAN OR GET FREE MEDICAL CARE.**

There are myriad ways for the bad guys to get your information and use it for all sorts of nefarious purposes—mainly, stealing your money, although occasionally for other kinds of fraud or to cover their tracks when committing additional crimes. That's one of the big reasons identity theft can be so devastating. If a criminal steals your credit card information, your bank will likely refund you the money that was lost. If the same criminal impersonates you to run an international child pornography ring, however, then your problems just got a whole lot worse... especially since many law enforcement folks aren't up on the latest types of cybercrime, so "that wasn't me" might not go over well.

How does it happen? We'll examine the many methods of identity theft in the pages that follow, and we'll also show you how you can protect yourself from being a victim or fight back if you already are. The methods of ID theft range from the seriously low tech (such as digging through your trash for unshredded financial documents or stealing those new credit cards that the bank sends you unexpectedly) to sophisticated database breaches and other hacks staged half the world away by

large crime syndicates to fund cyberterrorism operations.

**AMERICA'S FIRST IDENTITY FRAUD** Philip Hendrik Nering Bögel had some financial problems, and he was a creative thinker. So in 1793, when things got too hot for the Dutchman (who was wanted for embezzlement at the time), he did what any forward-thinking identity thief would do today: He hot-footed it out of the Netherlands, setting forth on this continent a new city, conceived in parsimony, and dedicated to the proposition that Bögel deserved better. Calling himself "Felipe Enrique Neri, Baron de Bastrop," Bögel started being awfully helpful to early Texas leaders Moses and Stephen F. Austin in obtaining land grants. After being named Texas land commissioner, Bögel came to settle a Texas city that he named after himself. Today, visitors to Bastrop, Texas, population 5,340, can celebrate how America's earliest successful ID fraud operation netted one guy a whole city.

**T/F**

## "MY IDENTITY ISN'T WORTH STEALING!"

**FALSE** Attackers are smart, and they seek the easiest path to their ultimate target. Often, that easiest path runs through your computer is you. You may say, "I just have photos of my grandkids on my hard drive." But your machine is connected to the internet, making it a target. Hackers can hijack your computer and join it into a secret global network for spam, attacks on other computers, and more nefarious activities. While they're at it, they might just steal

your banking information as well. It is also not unknown for hackers to destroy a computer, so that even those family photos that are priceless to you, while worthless to others, end up lost with the dead computer.

**MANY TYPES OF IDENTITY THEFT** Criminals impersonate you online for a range of different reasons and in a variety of ways. For cyberstalkers (see pages 50-51 for Amanda Nickerson's story), the impersonation is usually part of a larger cyberbullying effort. But in most cases, the motivations are financial. Whether it's designed to get bank cards or bank loans in your name, obtain credit in your name, or impersonate you to use your existing credit, identity theft is usually a gateway cybercrime—an initial act, atop which lie other criminal schemes. So really, "identity theft" should be thought of as a family, or a category, of cybercrime.

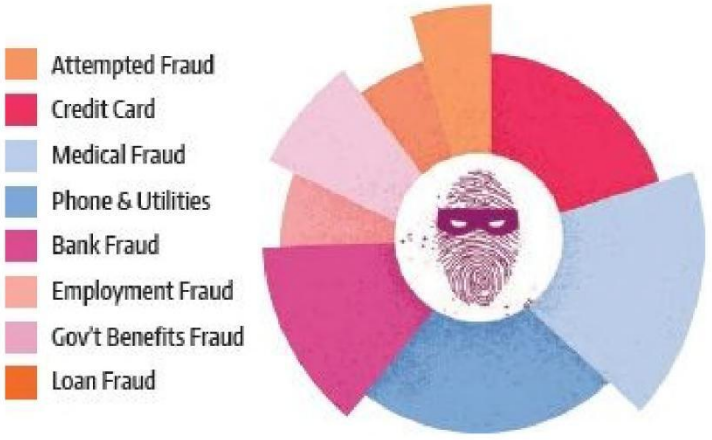
Even though it's common for victims to be reimbursed by banks or credit card companies, the damage done by ID theft can affect you for years. Your credit score and history are the main ways that banks, car dealers, and other lenders determine the risk of extending you credit, and the black marks can be hard to erase.

**A Taxing Scheme** One of the fastest growing crimes in America is tax return fraud, which can net identity thieves thousands of dollars for each successful impersonation they make to the IRS. The criminals get hold of your Social Security number and personal information, and then create a tax return in your name that shows a modest overpayment on your part. The return is filed online using software, and within days, the IRS sends out a refund to "you"—at the address given by the thief. The refund is

typically made using prepaid Visa cards, which can be easily exchanged for cash or property.

**FORMS OF IDENTITY THEFT**

Fraudsters don't just steal your driver's license or credit card. They'll take your whole identity and make use of any part they can.




## CASE STUDY

**STRANGERS WITH CANDY** In 2004, some InfoSec folks did a little experiment in which they offered passersby on the street a candy bar if they would tell them their work logins and passwords. To their surprise, some 70 percent were willing to part with the information—half of them did so even without the chocolatey bribe. You'd think that would have been a wake-up call. And indeed, governmental agencies and private-sector companies spend millions of dollars on training to make employees aware of proper

security procedures and how important it is to follow them. How's that going? Well, when the experiment was repeated in London in 2008, there was no difference.

Whether the reasons are cultural or technical, the fact is, people are just really bad at keeping their passwords secret. They just don't take it seriously. What's even more galling to those who work with companies and individuals to improve security comprehension is that "your password" is still taken literally. By which I mean that most people to this day use just one password for many or all of their accounts—and a weak one, at that (see page 28 for more on creating a secure password).

You might think that this problem would have already been solved with the creation of password manager apps, which significantly reduce the toil and trouble of thinking up (let alone remembering) strong new passwords, such as the ever-popular 98cLKd2rh29#@36kasgJ!. Plus, the programs are easy to use and can automatically change the passwords for all your online accounts.

So in 2016, when a security consultant decided to try the chocolate bar trick again, this time staging it as a contest in which the person with the "best" login and password would win prizes ranging from candy to a bottle of Champagne, he finally got different results: They were even worse than before.

## SECURITY BASIC

**GUARD THOSE DIGITS** You should think thrice before handing over your Social Security number (or, outside the

U.S., your national identity number), even if a legitimate office is requesting it from you. This number is a universal identifier, and you've probably been asked for it multiple times a year, every time you open a bank account, take out a loan, or verify your personal information. It always pays to think about why it would be needed and to refuse to provide it unless it is absolutely necessary. If you're paying cash, never give out the number. I would rather put down a $75 deposit to get electricity or phone service than provide the utility company with my Social Security number—plenty of utilities have been routinely hacked, and ID theft in America thrives on this ubiquitous identifier. If the service provider doesn't need it, don't provide it to them.

## TRUE STORY

**TINFOIL HATS** It's a common joke that some people are so paranoid, they line their hats in tinfoil. Funny thing? That might not always be such a bad idea.

There are many ways to conduct data theft, and some of them do rely on secret transmissions. The best (or, at least, one of the coolest) examples of this was the Soviet hack against IBM Selectric II and III typewriters in the 1970s. About fifteen of these were used in the U.S. Embassy in Moscow and the consulate in Leningrad, and were modified by Soviet spies to contain a device that measured the magnetic disturbances generated when the little Selectric ball swiveled. Each letter, it turned out, had its own signature. By implanting a receiver in the walls (the buildings were, of course, built by Soviet contractors), the

government could see the very pages of documents as they were typed up.

**HOW THEY DO IT** Criminals engage in obtaining identities to exploit in a range of ways, from low-tech to Secret Squirrel. Once the most common method of identity theft, paper or wallet theft is still popular, but now it's a small-time operation. Still, someone lifting your wallet and using your ID and credit cards can do a fair bit of damage. Similarly, ID theft can occur when people rifle through your trash and find bank statements and other bills with account numbers, balances, and dates. These specifics allow thieves to call those vendors and report your cards as lost, change your address, and have replacements mailed to them.

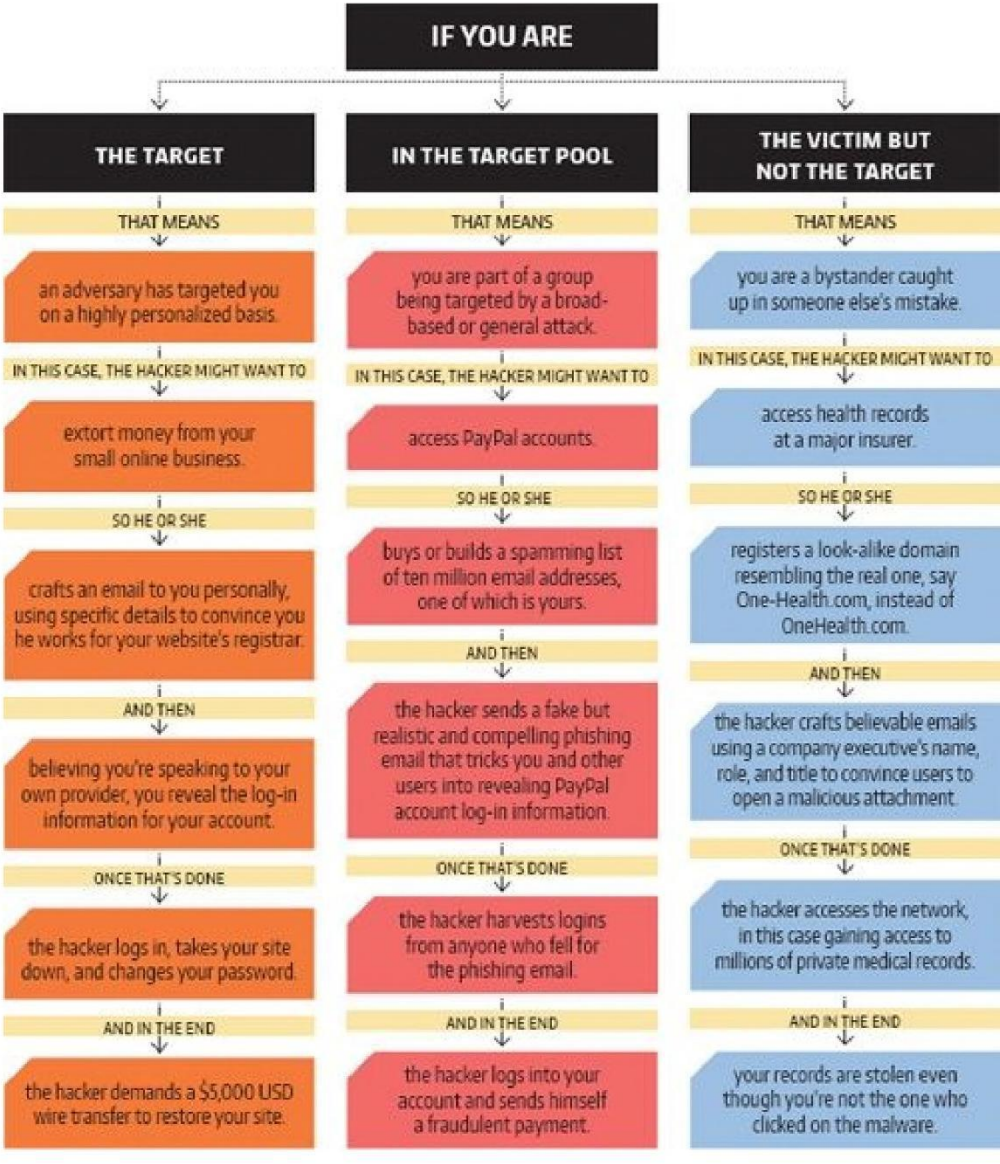
Other schemes to separate you from your identity run the gamut from physical theft of personal documents from service providers to breaking into a computer network specifically for the purpose of stealing data. Another popular method is phishing

(see page 24).

But of course, the most common method of stealing identities is to do so en masse in a large-scale breach of a retailer, bank, insurance provider, or government agency. This gives criminals the biggest bang for their buck and the largest number of targets. See the chart on the facing page for more information about how this works.

**One Step Ahead of the Law** It is very difficult for authorities to prevent or successfully prosecute identity thieves. Because much of the fraud can be done at a distance and by using online tools, catching the criminals in the act is difficult. What's more, with the global nature of the internet, the criminals don't even have to be in the United States to commit these crimes. And, finally, ID theft can go on for some time before a victim is even aware that it has happened.

**HOW MIGHT YOU BE VULNERABLE?** The vast multibillion-dollar cybercrime industry can be divided into three basic categories, each with its own objectives, although at the end of the day, the result is the same: You've been had. Understanding the differences, and what happens at each stage of the game, can help you stay safe. Here's how these crimes roll out.



## KEY CONCEPT

**WHY IS IT CALLED PHISHING?** Phishing is a term used to describe some of the most widespread and effective methods for obtaining information online. The term itself is a mash-up of two words—"fishing" and "phreak." The fishing part is just what you'd imagine: to fish for victims or data by using electronic bait, hooking victims, and reeling them in—an obvious and accurate metaphor for the act itself. The alternate spelling is a nod to the pre-internet practice of telephone-system hacking known as phone "phreaking," done by "phreaks." This is related to another hacker practice, called "'leet speak," which substitutes numbers for letters and some letters for others to create an often goofy insider jargon. It's quaint today, but you will still see versions in chat rooms, as hackers somewhat jokingly refer to one another as "133t H4×0r5," or "elite hackers."

**TEACH A MAN TO PHISH** Phishing isn't one specific thing. Rather, the term is used for a wide range of methods designed to gain access to your information. Understanding what those methods are, along with the basics of how they work, is central to both recognizing and avoiding many of the risks you face online. So before we go any further, let's do a quick overview of the many types of phish in the sea and the ways they can bite. Here are three common methods that these criminals will try when going after your data.

**Voluntary Disclosure** The first method is diabolically simple: Attackers use a rich mix of psychological techniques, known collectively as *social engineering*, to get you to give up the goods, essentially conning you into giving away the information that they want. People are generally trusting, and it's amazing how much information the average person will give up simply because someone happened to ask them in the right way.

**Malicious Attachments** In these cases, computer users are tricked by some compelling message into opening a poisoned email attachment, which then installs malicious malware on their machine, thus giving the hacker access to their computer or network. These masquerade as documents that the users "requested," photos they "just have to see to believe," and the like.

**Malicious Links** Because many email systems can now block out malicious email attachments, some attacks will use malicious links to drive the user to an infectious web page instead. Most people are so accustomed to clicking on links almost automatically that this technique is highly effective. Most of these links are disguised to boot—an image in the email with a

logo or a line of text displaying an address or site to visit that is actually a cover for a malicious web address which a hacker has set up for just this purpose.

**TYPES OF PHISH** There are a lot of phishing schemes in the sea. You've probably been exposed to at least a couple of the examples listed below—and hopefully you didn't fall for them, although if you did, you're one of millions of people who have. Using the information below, you'll be better able to spot these scams and steer clear.

**TYPE OF SCAM**

**CLASSIC PHISHING**

**HOW IT WORKS**

A fake website "spoofs" or closely resembles a real one, into which users enter their access credentials, identity data, or other sensitive information.

**SPEARPHISHING**

### HOW IT WORKS

As the name would imply, this is a highly targeted attack, often designed to victimize a small, specific group or even one individual, using highly personalized messages that may be the result of hours or even weeks of online reconnaissance on the target.

### WHALE PHISHING

### HOW IT WORKS

The spearphishing of a high-profile or high-value individual, such as a CEO or celebrity, that is, a "big fish" or whale.

### CATPHISHING

### HOW IT WORKS

The use of fake online personas or profiles to create a phony emotional or romantic relationship, either for financial gain or access to sensitive information.

### VISHING/SMISHING

**HOW IT WORKS**

Scams or data thefts that leverage phishing-like techniques but target phone users over voice lines or SMS.

**IF YOU'RE ENTERING PERSONAL DATA ONLINE, TYPE THE ADDRESS YOURSELF AND CONFIRM THE SITE IS SECURED WITH AN HTTPS PREFIX AND A CLOSED-LOCK ICON.**

**T/F**

## PHISHING EMAILS ARE EASY TO DETECT

**FALSE** A lot of people believe that they can easily tell when they're being phished through email. But more and more often, scammers are crafting messages that appear to be from a legitimate source, such as your bank or your Amazon or eBay account, complete with a full page of images and icons from those sites duplicating a genuine email—but secretly redirecting an unsuspecting user to another site. You can sometimes confirm it's a fake by moving your mouse over the link (without clicking) and seeing another address pop up in preview. But just to be on the safe side, you should always enter the address yourself, never by clicking links.


**DEFEND YOURSELF AGAINST PHISHING** So if the thieves are smart, and not even the rich and famous can protect themselves, does that mean you're hosed? Not at all. That's because in most cases, victims fall for these attacks not out of a lack of resources but a lack of awareness. An astute and informed user with a zero-dollar budget is harder to victimize than an oblivious and untrained one with all the money in the world. Here are five simple steps you can take, starting right now, that will make you a significantly tougher target for phishers.

**Be Aware** Simple awareness is the first line of defense. Be suspicious. Understand and believe that you are a target. Treat any message in any electronic medium from someone you don't know as highly suspect.

**Use the Hover Test** Any modern email program will show you the destination of a hyperlink if you mouse over it without clicking. This "hover test" can help you spot suspicious links in any email you've received. If the visible link and the underlying destination don't match exactly, don't click!

**Check the URL** Learn how to properly read a web address. The

name of the site you're visiting is the last thing to the left of the first single slash, not the first thing to the right of the double slash. Phishers constantly use this lack of knowledge to trick people.

**SAFE: https://www.amazon.com/**
**UNSAFE: http://www.amazon.phishingforyou.com/**

**Be Attachment Phobic** Malicious attachments are the number one way to let password stealers, Trojan horse viruses, and other nasties get onto your computer. You should only open attachments from people you know, and even then limit yourself to messages you're expecting, such as an invoice for services you actually have received.

**Confirm Out-of-Band** If you happen to receive a suspicious message or a request for information that seems too personal, even from individuals or companies you trust, confirm the request via a different medium. For example, if they email you asking for your information or requesting that you click the link to their website to correct an issue, try visiting their website or calling them by phone. And remember, type the web address out manually or find the phone number yourself. Never rely on the link or phone number in the suspicious message. Those could both be fakes run by the phisher!

## HACKER HISTORY

**PHONING IT IN** The first known online mention of the term "phishing" was in the online group alt.2600, a discussion forum for phone hackers, in early 1996. The "2600" refers to

the frequency in hertz that early phone phreakers discovered they could play into a phone handset to take over the phone company's switches and make free calls to anywhere in the world. That this hack was so simple to execute, and so fundamental to the system that it was simply too expensive to fix, led to an entire subculture around building "blue boxes," or tone generators that would play the 2600 Hz whistle tone. Even Steve Jobs and Steve Wozniak, of Apple fame, sold them in the early days. One intrepid phreaker, John Draper, worked with some blind phreakers who were, as you'd imagine, particularly sensitive to tone. He learned that a plastic whistle offered as a free prize in boxes of Cap'n Crunch cereal blew at, yes, 2600 Hz. Draper used the whistle widely and became known in hacking circles as Crunchman. He's still around, too: You can find him on Twitter @jdcrunchman, or look for John "Captain Crunch" Draper on Facebook.

## GOOD TO KNOW

**YOU'RE NOT ALONE** Millions of ordinary citizens have been victimized by one type of hack or another. Even the smart, powerful, and rich have been victims. For example, real-life rocket scientists at NASA have had their computers taken over by Chinese hackers. The U.S. government has concluded that Russians hacked the DNC and that Anonymous hacked Donald Trump during the 2016 election. In 2008, vice presidential candidate Sarah Palin's email was stolen by a hacker who figured out the Alaska governor's email password. Other notable victims have included

Attorney General Eric Holder, FBI Director Robert Mueller, Jay Z and Beyoncé, Paris Hilton, Mel Gibson, Kim Kardashian—and Nick Selby, one of the authors of this book. This isn't even taking into account the massive amounts of top-secret government information released by WikiLeaks, Edward Snowden, and others.

## KILLER APP

**CAN I TALK TO YOUR MANAGER?** The longest, most complex passwords are impossible for hackers to break in a lifetime (or even several!), but it also seems as if they might take a lifetime to come up with and nearly as long to input each time you have to use them. Luckily for you, there are password manager programs out there that can do all of the heavy lifting for you.

A password manager site or application like LastPass, Dashlane, or 1Password can generate, store, and encrypt a list of passwords for you, import any passwords that you have previously created yourself from browsers, analyze the strength of a password, and more.

Just be sure that you can remember and keep secure the master password to the account itself—and luckily, many password managers also offer two-factor authentication (see facing page) for an added layer of password protection.

**CREATE A POWERFUL PASSWORD** Now that you know what to avoid in emails, what's the next step? Well, every online account requires an account name (often derived from your own name or email address) and a password. The following guidelines can help you come up with passwords that are as unbreakable as possible.

**One Size Does Not Fit All** Look at the keys on a key ring: Each is a different design and cut. Just as each key is made to fit a specific lock, each password should be unique to the account it's used for. Otherwise, if you're a victim of ID theft, whoever stole your information will have access to every single account of yours that the criminal can think to try.

**Bigger Is Better** Some sites limit how long your password can be. While a long password may be hard to remember, it's harder for a hacker to break, even with brute-force methods (that is, using programs that try every single possible combination of characters).

**Get Complicated** Passphrases like "correcthorsebatterystaple" are easy to remember, but anything that uses dictionary words is easily hackable. Avoid simple substitutions, too, such as "p4ssw0rd" instead of "password." Use every single type of character you can: lowercase and capital letters, numbers, punctuation, and anything else available. Finding a number between 0 and 9 is easy for a hacker or ID thief; finding the right character in a total of sixty-two numbers and lowercase and capital letters is massively more challenging, especially the longer the string gets. If you have to write down a password to help remember it, keep said document hidden and safe from prying eyes or theft, or consider using a password manager.

**Change Is Good** Don't just come up with a password and then leave it be. Change your passwords frequently and, if at all possible, never reuse one. If hackers steal older data, they may score a hit if you're using that old password for a new account.

## SECURITY BASIC

**JUST DON'T** The top ten most common—and thus worst—passwords have stayed largely the same since passwords became a thing, only changing in order from year to year. Right now the top contenders are:

1. **123456**

2. 123456789
3. 111111
4. qwerty
5. 12345678
6. password
7. 123123
8. 000000
9. 1234567
10. 1234567890

**WHO WANTS TO KNOW?** Sometimes an extra layer of protection, called "knowledge-based authentication," or KBA, is added to your password, either in addition to your basic login and password or to verify your identity if you've forgotten your password. Of course, like many other defenses, this tool can also be turned against you.

**Static KBA** Also known as "shared secret questions," these are questions along the lines of your mother's maiden name, town where you were born, and so forth—often matters of public record. In addition, this information is stored somewhere, so it can be stolen, which means that even the weirder questions, like "Who's your favorite poet?" aren't secure.

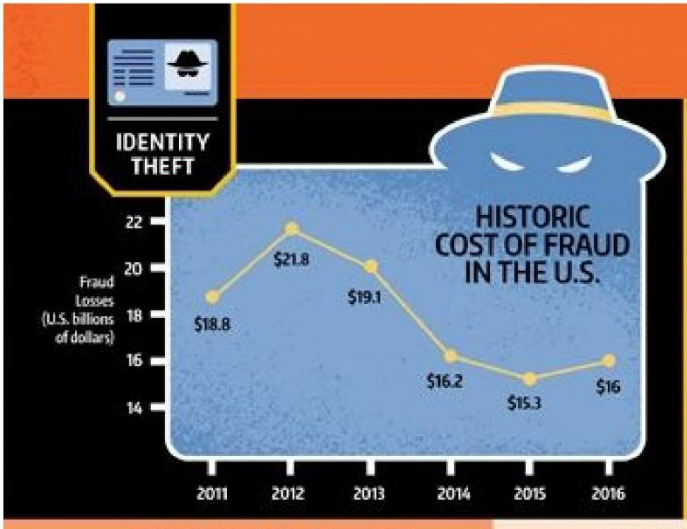
**Dynamic KBA** Here, questions are generated in real time from a range of public and private records. You don't know what questions will be asked, but, hopefully, you'll remember the answer. Examples might include "What color was your Honda

Accord?" or "Which of these streets have you never lived on?" You only have a short time to answer; the odds of someone guessing correctly on the fly are lower.

Unfortunately, you may not have the luxury of only patronizing sites with excellent dynamic KBA, although if you have the choice, take it. The simple workaround? Lie. It's relatively easy to figure out where someone went to high school. But if the "correct" answer is Narnia, Petticoat Junction, or Westeros, that's less likely to show up in old yearbooks. More's the pity.

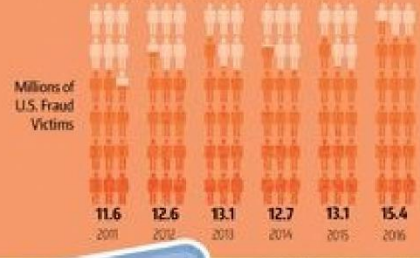
## SECURITY BASIC

**USING THE POWER OF TWO** Two-factor authentication, also called "2FA," is like a counterpassword in a spy novel ("The blackbird sings at midnight"; "But only under a full moon") or two people turning keys at the same time to launch a missile. Often available as a mobile app or a physical token (something like a key ring tag) that only you would have access to, 2FA uses a shared algorithm attached to your account. After typing in your password, you're prompted to use the app or push a button on the tag to generate the authentication key based on that algorithm, usually a short string of numbers randomly created on the spot. If an account offers 2FA (such as Google Authenticator), use it, and your accounts will be that much harder to compromise. If you should lose the token or the mobile device with the app, replace it ASAP so you can keep your account safe.

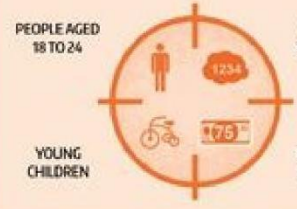



**90%** OF VICTIMS REPORT THEY WEREN'T EVEN AWARE THAT THEIR PERSONAL DATA HAD BEEN COMPROMISED BEFORE THIEVES TRIED TO USE IT FRAUDULENTLY.

## GROWTH IN CASES OF ID FRAUD




## THE MOST TARGETED GROUPS





## COUNTRIES WITH HIGHEST INCIDENCE OF IDENTITY THEFT PER CAPITA

1. MEXICO
2. THE USA
3. INDIA
4. THE UNITED ARAB EMIRATES
5. CHINA
6. THE UNITED KINGDOM
7. BRAZIL
8. AUSTRALIA
9. SINGAPORE
10. SOUTH AFRICA
11. CANADA

**64%** Credit cards that showed attempted or successful use by thieves.

## IF YOUR PERSONAL INFORMATION IS STOLEN, HOW LONG DOES IT TAKE TO RESOLVE?

| | |
|---|---|
| 48% | 1 DAY OR LESS |
| 16% | 2 TO 7 DAYS |
| 18% | 8 DAYS TO A MONTH |
| 6% | 1 TO 3 MONTHS |
| 3% | 3 TO 6 MONTHS |
| 9% | 6 MONTHS OR MORE |

## SIGNS YOUR IDENTITY HAS BEEN STOLEN

- YOUR CREDIT CARDS RATES GO UP
- YOUR CREDIT RATING DROPS
- MYSTERY BILLS SHOW UP
- CAR INSURANCE GOES UP
- BANK STATEMENTS STOP COMING
- TAX REFUND DENIED
- CAN'T RENEW DRIVERS LICENSE
- CHECK-UP REMINDERS FOR MEDICAL CONDITIONS YOU DON'T HAVE
- CALLS FROM COLLECTION AGENCIES
- TURNED DOWN FOR LOAN
- FAIL TO PASS BACKGROUND CHECK FOR JOB

## 30 DAYS

Average time needed to handle identity theft crime.

## MOST COMMON FORMS OF IDENTITY THEFT

| 49.2% | 15.8% | 9.9% | 5.9% | 3.5% | 3.3% | 22.9% |
|---|---|---|---|---|---|---|
| ATTEMPT TO ACCESS GOVERNMENT DOCUMENTS* | CREDIT CARD FRAUD | PHONE OF UTILITIES FRAUD | NON-CREDIT CARD BANK FRAUD | LOAN FRAUD | EMPLOYMENT-RELATED FRAUD | MISC OTHER FORMS |

*ID, social security number, tax returns, etc.

## 30 HOURS

Average time to handle and settle a disputed charge with a credit company.

## GOOD TO KNOW

**SCURITY BASICS** Your wallet often has all of your identification and bank cards (and more). If that wallet gets stolen, your entire life's identity and finances will literally be in someone else's hands. Should that happen, the best plan is to have culled its contents well beforehand so that you're only carrying the minimum number of IDs and credit cards—nothing more than is absolutely necessary. This will limit your losses in case of theft. And, it means that the only calls you will have to make will be to your credit card company, your local DMV office, and your employer to report the losses. Your credit card and driver's license will be replaced, and your employer can deactivate your work ID card, thus preventing whoever stole your wallet from using the card to break into your office and clean you out of paper clips and printer ink cartridges.

**THE SEVEN-POINT ID THEFT RECOVERY PLAN** If you have been the victim of identity theft, it is very important that you take steps to safeguard your good credit, warn the appropriate agencies of the event, and protect your good name. Often, you'll want to talk to the police. That's a good idea, but don't be surprised if you learn that there's not a lot they can do. The rest of this chapter explains how you can help yourself when you are the victim of identity theft. If you don't, it can cost you dearly when applying for a car loan, mortgage, or credit card. It could also make it harder for you to find a job, rent an apartment, or buy insurance.

The first thing you must do when you are a victim of identity

theft is to get organized. The seven-step checklist here is just a suggested series of steps; customize it as necessary to your needs.

**STEP 1**

**FILE A POLICE REPORT**

If you discover you have been victimized, contact the non-emergency number of your local police department and ask to speak to a detective.

**STEP 2**

**GATHER DOCUMENTS AND EVIDENCE**

Contact your nation's consumer protection agencies, as well as stores and creditors to gain copies of the documents used to open accounts in your name.

**STEP 3**

**CREATE AN AFFIDAVIT AND ID THEFT REPORT**

Your local consumer protection agency should be able to provide documents you will need and demonstrate how to present them. They also provide sample forms for an identity theft report, which, along with your police report, will help speed up the process with creditors, banks, and other agencies.

**STEP 4**

**INFORM THE CREDIT AGENCIES AND CREATE AN EXTENDED ALERT**

To establish a fraud alert with the credit agencies, contact them directly. You will need to reissue the alert every ninety days.

**STEP 5**

**INFORM YOUR BANK, CREDITORS, AND MERCHANTS**

With the package you've created, contact your bank and other creditors and merchants with whom you have accounts and inform them of the issues you have faced.

**STEP 6**

**PROTECT YOUR SOCIAL SECURITY NUMBER**

If your number was misused, inform the national agency and request information on an ID Theft Affidavit. You may also wish to contact your agency if your Social Security number is being continually abused or phone to victims of identity theft.

**STEP 7**

**MONITOR YOUR CREDIT**

You are entitled to at least one free credit report per year, but that is often insufficient for monitoring. There are several commercial companies offering these services, and we recommend you seek professional advice on which to choose. Several nonprofit organizations are out there to help victims, offering assistance to victims of identity theft by internet or phone.

**SHRED AND THOROUGHLY DESTROY ANY OLD AND UNUSED CREDIT CARD APPLICATIONS OR SIMILAR FORMS TO HELP KEEP YOUR INFORMATION OUT OF THE HANDS OF ID THIEVES.**

**IF YOU HAVE CHILDREN, PRIVATIZE AS MUCH OF THEIR INFORMATION AS YOU CAN, AS THEY ARE THE GROUP MOST VULNERABLE TO SYNTHETIC ID THEFT.**

**SYNTHETIC ID THEFT** This chapter deals with the theft of someone's actual identity, but here's a new twist: synthetic identity theft. That's when an identity that has never before existed is created by scammers. Identity thieves typically seek to obtain names, national identity numbers and dates of birth, medical account numbers, addresses, birth certificates, death certificates, passport numbers, bank account or credit card numbers, passwords (like your mother's maiden name or children's or pet's names), telephone numbers, and even biometric data (such as fingerprints or iris scans). With synthetic ID theft, thieves only need some of this information to create a whole new fake person.

Thieves then create a credit file—the closest thing in the digital domain to conjuring up a human. This exploits a weakness in the authentication scheme used by credit reporting agencies: If an identity doesn't exist when it is checked, a new file is created. And a file? That's gold.

**Credit Where No Credit Is Due** The best thing to do with a synthetic ID is build its credit over time. This can be done in the traditional way—almost anyone can get a high-interest, low-limit, unsecured credit card at a hardware store, so the idea is to get one, then buy a hammer and pay it off over time. To get fancier about it, they might join up with a "data furnisher" who works at a business and will write up a phantom credit account for our spooky friend, showing scheduled payments made over time to speed things up. There's an entire industry around this, because the stakes are very high.

The most common way is to conjure up children. This is because, for the eighteen years or so after most kids are born, they don't do anything with their credit. During that time, anyone who establishes a credit file for the young one in question would likely be free from any interference until someone notices—that's typically at just about the worst time: when the kid applies for a college loan. The best way to protect against misuse of your child's credit is the same as it is for yours: Check it regularly, and check on it as often as you can. Should you happen to see fraudulent accounts, yell early, often, and loudly.

If you are on active duty in the military, it is recommended that you put an active duty alert on your own credit files by contacting any one of the three major credit agencies. Credit agencies all share active duty alerts. Each alert will stay in your files for at least twelve months. If someone applies for credit in

your name, creditors will take extra precautions to make sure that the applicant is really you.

### THE TAKEAWAY

Here's how to apply the lessons of this chapter, whether you're looking for basic safeguards, enhanced security, or super-spy measures to safeguard your privacy.

### BASIC SECURITY

- Use strong passwords.
- Use different passwords for every site.
- Use a password vault program.
- Never share your login information with anyone.
- Don't click on suspicious links or download unexpected files.

### ADVANCED MEASURES

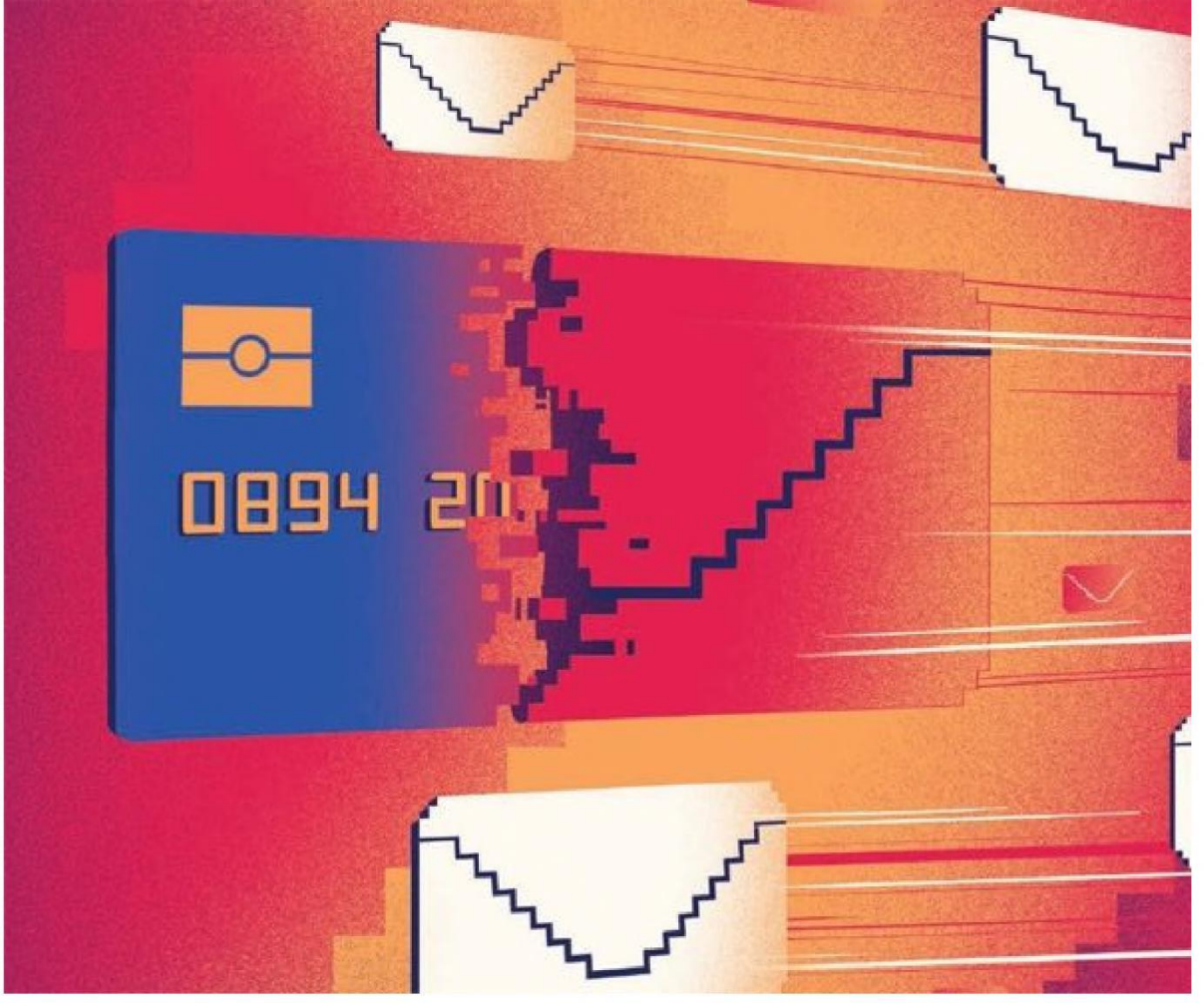
- Always use two-factor authentication.
- Don't get kids social security cards unless necessary.
- Check your kids' credit at least quarterly.

### TINFOIL-HAT BRIGADE

- If any service provider's site uses weak KBA, take your business elsewhere.
- File your taxes the old-fashioned way, on paper.
- Eschew electronic information wherever possible.

## GOOD TO KNOW

**WHAT LAWS PROTECT YOU?** In virtually every place you care to look, identity theft is considered a federal crime. But it can still be next to impossible to actually get a federal office to investigate your individual case of identity theft—well, unless you are famous, or rich, or there is something larger at stake connected to the theft itself. Most states have their own laws against identity theft as well, and your local police department may have a program that can help you—ask them what resources are available in your area. Ultimately, however, you may simply be on your own, as it can be difficult to track down a specific perpetrator of identity theft (especially given that you may just be one of many victims caught in the same sweep). Usually, the best you can do at the local level is work to limit the damage done and clear your name.



CHAPTER 2

# WHERE THE MONEY IS

**THERE IS MONEY IN CYBERCRIME. NOT "BUY A NEW CAR" MONEY. NOT "BUY A NEW HOUSE" MONEY. THIS IS "BUY A NEW AIRPLANE" MONEY, MAYBE EVEN "BUY AN ISLAND" MONEY. OF COURSE, IT'S MONEY THAT BELONGS TO YOU.**

In his autobiography *Where the Money Was: The Memoirs of a Bank Robber*, America's most celebrated bank robber, Willie Sutton, denied ever saying that he robbed banks because "That's where the money is." Nonetheless, it's a great line. And for cybercriminals, it's a directive. Where is the money these days? On the internet. Even garden-variety spammers and botnet managers can expect to bring in $20,000, $30,000, even $50,000 USD a week. If you're bad at it, you'll make less. If you're good at it... well, the FBI said that the hacker and criminal-empire builder known as Dread Pirate Roberts was earning $1 million USD per week before his arrest. That's seven dollars and fourteen cents every second.

And you don't even have to be a criminal to pull down big bucks from hacking—even the so-called "white hat hackers" (also called "ethical" hackers) can have a payday, too. The FBI is said to have paid a cool million for the hack that enabled the bureau to access the iPhone belonging to one of the suspects in the 2015 San Bernardino mass shooting, and in September of 2016, *Wired* magazine reported that a high quality, previously unknown iPhone hack had been sold for $1.5 million USD.

In short, both bad guys and good guys hack... because that's

where the money is.

**SUCH A NICE BOY** By all accounts, Maksym "Maksik" Yastremskiy is a nice boy. The twenty-five-year-old baby-faced Ukrainian was fun and friendly, and he bought nice things for his mother. He could afford to because in just about a year, young Maksik cleared some $11 million USD selling credit cards he and his friends stole from T.J.Maxx, an American retailer, before he was busted. Maksik's accomplice, Albert Gonzalez, was arrested as well. Perhaps suspicious of banks, Gonzalez had buried a barrel containing $1.1 million in cash in the backyard of his parents' home. Cops seized other fruits of Gonzalez's work, in the form of a new BMW, a condominium in Miami, his ex-girlfriend's Tiffany diamond, and three Rolex watches. So great were the stacks of cash he netted, Gonzalez bought himself the kind of currency counter used by bank tellers and casino cashiers.

**NEVER REPLY TO ANY EMAIL THAT CLAIMS TO HAVE BEEN SENT BY YOUR BANK AND IS ASKING FOR YOUR ACCOUNT INFO. INVARIABLY, IT'S A SCAM.**

**THE ELECTRONIC ECONOMY** When the average person thinks of the economic side of cybercrime, what comes to mind is theft... someone stealing your credit cards or other funds electronically. And, indeed, this is a massive business, with some $15 billion USD

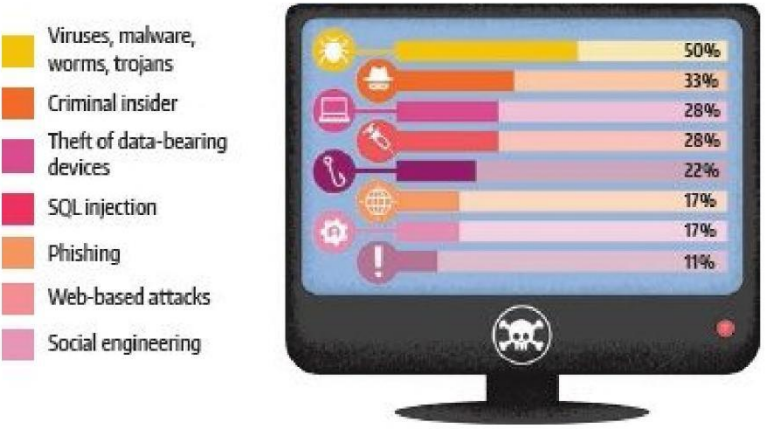
stolen electronically every year. However, there are other sketchy ways that money changes hands (or flies out of your wallet) online. In this chapter, we'll examine a number of them—and how to protect yourself.

**Identity Politics** Often times, a phishing expedition or other sort of identity theft is just the first step in a series of attacks. While an identity thief may use data stolen from you for a number of purposes, as discussed in the previous chapter, the most common is to steal your money or use your identity as a shield for a larger theft. That's why it's so crucial to do your due diligence when you discover identity theft or fraud. After all, your credit card will almost certainly refund any fraudulent charges as long as you promptly report the card missing and file a police report, if required. However, if the thief then goes on and uses your identity to front a multimillion-dollar international con game, that would be a little less easy to resolve with a call to your local customer service rep.

**Shady Sales** Criminals don't have to steal your identity to get their hands on your money. You might be willing to hand it to them with a smile. We'll talk about the deep end of unofficial online markets in future chapters, but know that you don't have to be buying an AK-47 or a kilo of heroin to be part of the underground economy. It can be much more mundane on the so-called gray market.

**DATA THIEVERY**

There are a multitude of ways that criminals can steal your data, from hacking into computers to pulling confidence scams.




**NOT THAT KIND OF TRADING CARD** As we were finishing writing this chapter, Nick's wife had data skimmed from her credit card. Since she checks her bank records regularly, she caught it the next day. The online history showed what are called "test swipes"—some $1 transactions, followed by a $49 test (many shops don't run authorizations or need a signature for purchases under $50), and soon after, a $599 purchase from Bed Bath & Beyond.

Her card data (the information in the magnetic stripe on the back of the credit card) had been grabbed by a fraudulent card reader. This data, known as a "dump," was gathered up with others into a pack and sold to a thief. This person downloaded the data and encoded it to another magnetic strip, such as the one on a hotel card key, which then would swipe just like the original card. Once we cancelled the card, the person using the stolen data dump breathed a sigh of regret, tossed the now-dead card on the floor, removed another from a stack of about a hundred they'd encoded from different numbers in the pack, and

swiped again.

## SECURITY BASIC

**ELDER FRAUD** A particularly cruel form of cyber theft targets the elderly. Every year, American senior citizens lose $2.9 billion to financial fraud. A study published by the National Health Institutes concluded that, basically, the older you get, the more susceptible you are to scams. Age was a stronger predictor than financial acumen, wealth, education, or health.

That's why so many online scams target the elderly. The over-seventy set is less likely to be computer savvy and thus falls prey to the "tech support phone call" scams, in which a helpful young man informs you that your computer has been malfunctioning; for just $29 USD, he can fix the problem. All he needs is a credit card number. This scam also manifests in a more aggressive form, as an "IRS auditor" calls to demand an immediate payment on mysterious back taxes. Wherever in the world you're located, you can find helpful tips on spotting and fighting common scams at the American Association of Retired Persons' website, updated monthly as new scams emerge.

## FUN FACT

**WHAT'S MY IDENTITY WORTH?** In brief: not much, despite the damage fraud does to you. The aftermath of an identity theft can take around thirty hours' effort to repair, with

losses averaging about $4,000 USD. But to an ID thief, you're just a drop in the bucket. A single dossier of a person's full financial and personal info might sell for about $1,300 to an interested buyer, but identity thieves often buy and sell in bulk. Files full of medical insurance info cost maybe a little more than $5 per stolen identity, while tens of thousands of Social Security numbers can be sold for as little as a penny per victim—so that list of 100,000 stolen SSNs (including yours?) goes up on the black market for just a grand.

## KEY CONCEPT

**FIFTY SHADES OF GRAY MARKET** Most of us have at least heard of black-market goods. But what about the gray market? Both gray- and black-market goods are purchased outside of the usual channels, compared to white-market (totally legit) merchandise. The difference is legality: Gray-market items may be technically legal, such as single items sold from a bulk pack or merchandise sent from a cheaper to more-costly region (such as from Scandinavia to the United States).

Gray becomes black, and thus totally illegal, when goods

are faked or counterfeited. It's often hard to tell whether you're getting the real deal or if that "Viagra" contains an overdose of the drug or nothing but blue printer's ink and plaster. Some black-market items are even malicious or actively harmful and thus considered red-market.

**WHAT ELSE IS ON SALE?** A comprehensive list of all the merchandise in each market out there would take up volumes. But here are some examples of each (we'll get into the more serious stuff in Chapter 12).

**White Market:** Taxed, licensed products and services; whatever you find on your local stores' shelves or on mainstream commercial sites like Amazon

**Gray Market:** Untaxed legitimate products; taxed but unlicensed products; smuggled cigarettes or medicines, used merchandise resold as new; certain imported vehicles

**Black Market:** Illegal unlicensed sales: counterfeit merchandise, stolen identities, drugs, weapons, fake IDs

**Red Market:** Illegal offerings actively causing physical harm: murder-for-hire, arms trafficking, slavery, child pornography

**I KNOW A GUY WHO KNOWS A GUY** That new game you wanted for your console this holiday season? It's now so in demand that it's on back order at the local department store, but your buddy knows a guy who works in the stockroom, and he knows when the next shipment is coming. What about that all-important textbook for your daughter's last college course? It's nearly worth its weight in gold at the university bookstore, but her roommate got a copy from Indonesia on eBay at a fraction of the cost! Maybe you need a new fridge, and you can't afford to shell out full price, but your friend says he can get you one, cheap—it just fell off the back of the truck when being unloaded is all...

These, in a nutshell, are gray-market goods: They're still legal, and you're still paying for them, but you're not exactly getting them through regular channels.

**Just a Little Shady** It's not quite a crime to possess or buy gray-market goods. Most goods for sale through these channels have been rerouted from different markets (so taxes may not have been paid on them), and trying to find them is sometimes

sketchy, but they're the genuine article nonetheless.

**Staying Safe** Most gray-market merch is perfectly normal, but some shadier dealers will sell pre-owned items as brand new or offer defective merchandise without letting you know. If your "new" game console conks out on you, you're out some scratch and probably more than a bit frustrated—but if that scuffed-up box of "new" brake pads turns out not to give your brakes enough grip at the wrong time? *Caveat emptor* is the phrase that comes to mind.

## GOOD TO KNOW

**TOO GOOD TO BE TRUE** The internet is full of knockoff and counterfeit goods. Here are some common examples.

**Clothing and Fashion Accessories** Because they are low tech and easy to make, brand-name fashions, watches, handbags, and other often-pricey accessories are massively counterfeited all over the world.

**Footwear** By some estimates, when you combine fashion and athletic shoes, brand-name footwear is the most counterfeited product category in the world, with fakes making up as much as one pair in ten worldwide.

**Consumer Electronics** A smartphone or PC might seem like a hard thing to copy, but it isn't for the thousands of firms that supply the same parts to the legitimate manufacturers.

**Health and Beauty Products** Gray-market sales of health and beauty aids run to 20 percent of authorized sales in

most markets... and as high as 50 percent of authorized sales in some. That may seem harmless, but knockoff makeup and toiletries can cause severe allergic reactions, so shop accordingly.

T/F

## TONER IS WORTH MORE THAN GOLD

**TRUE** Toner cartridges for your laser printer are ridiculously expensive, and most of what you're buying is the cheap plastic casing. The cost, and the value to the consumer, is in the few ounces of toner inside. Online fakes routinely sell for 10 to 20 percent of retail but could destroy your expensive printer. Don't risk it. Another example of these economic forces is that of cigarettes. Highly taxed, simple to produce, and high-value by weight, cigarettes are perfect for counterfeiting. Do counterfeiters take advantage of this? Well, consider that border authorities in the UK intercept an average of one million counterfeit cigarettes—every single day.

**GRAY-MARKET ELECTRONICS MAY SEEM LIKE A GREAT DEAL, AND THEY CAN BE, BUT THINK LONG AND HARD ABOUT HOW MUCH YOU'RE GIVING UP BY NOT GETTING THE WARRANTY, SERVICE AGREEMENTS, AND SO ON.**

**TAKING A GAMBLE** So, what if you see an item that's almost certainly too good to be legit, but you're willing to turn a blind eye to the writing on the wall for a really, really good deal? From an ethics standpoint, you're on your own. We're not going to tell you it's ever okay to rip off the original manufacturers or sellers—after all, if everyone just photocopies this book and sells the copies on eBay, we'd be out of work. That said, here's the spectrum from "don't do it" to "really, really don't do it." The answer actually depends on what you're trying to avoid. Here's a good framework for how to think about making safe, informed purchases on the internet.

**Rolling the Dice** If you don't mind buying a cheap knockoff of designer fashions or accessories, you'll find a wealth of them online. Just understand that copies can range from totally worthless junk all the way up to identical goods made by contract suppliers on the same production line as the originals. If you understand the risks and feel like taking a chance, the worst you'll do is waste some money on a really obvious fake "Katey Spadde" handbag.

**Watch for Counterfeits** Some items are so prone to counterfeiting and knockoffs that, if you must buy online and want to ensure they're real, buy only from reputable sellers. Shoes from Zappos, toner from Staples, car parts from AutoZone, or CDs from Amazon are likely fine due to the strict controls used by these major retailers. The same goods from unknown sellers on eBay or Alibaba are almost certainly fake. That's okay for stockings, less so for your auto parts.

**Never Ever** Some things you should just never buy sight unseen online. This list includes significant assets, such as cars, boats, real estate, and so forth, which likely won't exist when you try to claim them; high-end jewelry; and prescription drugs or anything else your health or life might depend on.

## CASE STUDY

**BIG SCAMS** One astonishing blunder was made not too long ago by an English bank that decided to save money by encrypting just the "sensitive" parts of its database. So, instead of properly safeguarding it all, they only did the "account number" and "date of birth" fields and such. And then thieves broke in through the bank's online banking application and sucked down the whole database. About three weeks later, customers began receiving letters on beautiful, cream-colored bank stationery, addressing them by name and referring to their account with that began with the numbers 271 (hint: all that bank's accounts did). "Dear customer," it read, "We value your business and want to make your online banking experience as good as it can be. Enclosed is a CD-ROM to help you! Just place the CD-ROM

into your computer...” Of course, the CD-ROM was a combination of keylogger, fake-online-banking, and man-in-the-middle applications.

Another big-bucks scam relies on employees being scared of offending a top executive. Because bosses can’t stop posting to social media, like, ever, scammers can track their movements through updates (“Just got to Shanghai, great meetings with ProX. Check out these offices!”). An employee then gets an email reading “Hey, Louise,” I’m here in Shanghai and I just met with ProX Printing. Apparently, we didn’t get their invoice three months ago and they are furious. Please send a wire transfer first thing this morning to...” The then boss provides a banking routing number and an account number. This scam is a highly effective spearphish, because it relies on so many things that seem like private data but are actually public. It works. Often. To prevent it, ensure that wire orders always—always!—follow the same verification process, by voice and with backups like second authorizers.

## SECURITY BASIC

**MOBILE BANKING** As easy as it is to use your mobile phone to check your bank balance, pay bills, or transfer funds, you should still be wary, or even dispense with doing mobile banking entirely if you can. Aside from the obvious risk of losing your phone or having it stolen with any pertinent personal info on it (especially if you happen to have left it unlocked and unencrypted), there are two major issues with mobile banking: The apps offered by most banks do not

support two-factor authentication (see page 29), and furthermore, many of the apps will accept any sort of security encryption info—even false info that a hacker can use for a man-in-the-middle attack on the bank's security (wherein a hacker intercepts, alters, and relays information sent between you and your bank)—and thus the security of your own account as well.

## HISTORIC HACK

**YOUR GUILTY SECRET** One gambit that surfaces every so often is the story of the "hitman with a heart." It goes something like this:

"You don't know me, but I am writing to you because, even though I am a professional hitman with scores of kills to my name, I feel sorry for you. Don't even bother trying to trace this email or going to the police; it won't work. All you need to know is, someone who knows you wants you dead. I have been paid $5,000 to kill you. But you're such a good person, so I want to give you a chance. I was given $2,500 down, and I get another $2,500 after you have been 'taken care of'. But I'll make you a deal: If you pay me the $2,500, I will simply go away. I will not kill you."

You have to wonder: do these crazy schemes actually pay off? Given that they pop up over and over, they must pay off often enough that some people keep trying them, it would seem.

**LOSING CONFIDENCE** Historic confidence games, such as the Spanish Prisoner, were the inspiration for a deluge of emails that

flooded the early internet. In the pre-internet days, this sort of con took some effort and time, and of all those envelopes mailed out by con men only a very small percentage found a gullible mark with money to spare. The internet changed everything—it turns out the only barrier was one of scale. Suddenly, hundreds of thousands, if not millions, of emails could be sent with very little effort or cost, and the 1 percent hit rate went from the occasional celebration to a sustainable business model.

**The Nigerian Prince** The most enterprising of these scammers were located in Nigeria. Spurred on by the internet, an exotic-sounding locale, and some early success, boiler room operations sprung up throughout that country, with dozens of employees acting as princes. The Nigerians became so synonymous with these kinds of scams that most people in the business still refer to them as "419 scams"—419 being the chapter of the Nigerian criminal code that bans fraud.

**Stranded in London** One modern scam takes advantage of how common global travel has become. The "Stranded in London" gambit begins with someone hacking into your email address book and harvesting all of your contacts. Each is then sent an

urgent message saying that while on a trip to London you were arrested or mugged or injured and hospitalized. The story varies but always ends with a desperate plea for the recipient to wire money immediately. The same virus that steals the contacts also shuts down the email account, so you don't see the emails from concerned friends and family asking whether you're okay, how you got to London, and which hospital you're in. Versions of this are also used after takeovers of Facebook accounts.

**The Spanish Prisoner** On March 20, 1898, the *New York Times* warned Americans of a new scam: It appeared that a "robber and a humbug" was sending letters to Americans from Barcelona. The writer was in prison on political charges, but, thankfully, through hard work and thrift he had managed to squirrel away $130,000. Now, he wishes to enlist the help of an honest American, you (of whom he learned through a mutual friend of great character, whose name he will, out of an abundance of caution, not mention), to help spirit this sum to America so that his beautiful daughter can marry her true love. If only you would facilitate this transaction, a third of the sum is yours to compensate you for your time and difficulty. If you could, by placing in escrow a mere trifle—say, $100—to show your good faith, the transaction can proceed.

If this sounds familiar, it's because the Spanish Prisoner is the basis for the entire family of confidence swindles known as "advance-fee fraud." As you can see, this isn't exactly new—the *Times* article pointed out that the scam was—in 1898—already an

old one.

**THE TAKEAWAY**

Make sure your money stays in your pocket (or your bank account or online wallet) by taking the measures below—at the very least you must apply the basics.

**BASIC SECURITY**

- Follow up on mystery bills or collection calls immediately.
- If you lose your wallet, report aLL cards missing immediately.
- If you get a text or email from your bank asking you for info, call a branch to make sure it's legit.
- If a get-rich-quick scheme seems too good to be true, it almost certainly is.

**ADVANCED MEASURES**

- Check your credit report regularly.
- File a police report after fraud of any amount.
- Only use CHIP-and-signature cards (or CHIP+PIN when available).

**TINFOIL-HAT BRIGADE**

- Don't use banking apps on your phone
- Don't shop online.
- If a store only has swipe machines, take your business elsewhere.

## KEY CONCEPT

**CONFIDENCE SCHEME** The idea behind every one of the scams you'll find within this chapter, from the historic to the modern, from the in-person grifter to the fictional Nigerian banker or prince halfway around the world, is the idea of the "con." These scammers are working to gain your trust in order to convince you to bring them into your confidence (hence the term) and to make you believe that their sob stories or their threats or their bribes are true. As the old saying goes: "If the story sounds too good to be true, it probably is."

Before you react right off the bat—whether you're doing so out of charity, fear, or a desire to get in on the riches—take a moment to pause, think it over, and spend a few minutes to do some research. More often than not, you'll discover that it's just another con and shouldn't be trusted.

CHAPTER 3

# PROTECT YOUR PRIVACY ONLINE

**MORE AND MORE OF YOUR PRIVATE LIFE IS AVAILABLE ONLINE EACH DAY. YOUR WORK CONNECTIONS, YOUR SOCIAL MEDIA PROFILE, AND THE PHOTOS ON YOUR PHONE ARE IN THE CLOUD, MAKING YOUR LIFE AN OPEN BOOK TO CRIMINALS.**

As high-speed internet connections become available around the world, more and more of our lives are migrating online. People keep their résumés on LinkedIn, tweet links to their Instagram feed, and use Facebook for pretty much everything. And those photos and videos that used to eat up your hard drive space? You stashed those online, right? After all, if everything is password protected, it must be secure! That's the promise of "the cloud," a fluffy name for a network of servers on the public internet that let you stash your private documents, photos, and more. Imagine a massive train station with multiple banks of lockers. Anyone can enter the station, but if you stash your valuables in a locker, only you have the key that can open it—until someone secretly duplicates your key (i.e., steals your password) or just pries it open with a crowbar (i.e., uses malicious code that compromises your private files).

The cloud is growing every day—and not just with private files. Massive companies such as Amazon, Microsoft, Google, and others are migrating from earthbound data centers into cloud systems, too. In other words, a lot of private data is going into a public space. If the last two chapters have taught you nothing

else, it should be that this trend is like catnip for cybercriminals.

**NOTHING TO HIDE** One of my friends is fond of saying, "Unless you called the police, don't talk to the police." He happens to be a thirty-year veteran police commissioner who probably knows what he's talking about. Why is this relevant here? Because the idea that "I haven't done anything wrong, so I don't need to worry about being hacked" is about as naive as the thought that "maybe if I explain to the officer that those drugs weren't mine, he'll let me go." So, why should you lock down your Facebook profile when all you post is pictures of your cat? Because that open-book page is easily hijacked. The next thing you know, Mrs. Whiskerson is wanted by Interpol for money laundering. Or a hacker using your name and email is asking all of your friends for a $100 USD loan. Guard your social media and other online accounts as carefully as you would other information.

## GOOD TO KNOW

**FROM RUSSIA, WITH SPAM** So assuming that the Russians, in some form or another, hacked the 2016 election in the United States, how did they do it? The size and complexity of the scheme is still being discovered, but here's one piece of it. Democratic candidate Hilary Clinton's campaign website was likely attacked by a Russian-linked criminal group using a targeted spearphishing barrage designed to look like it came from the Clinton campaign. The campaign's email system was breached, and those emails went out to

her supporters. A whole lot of people who received those bogus emails clicked on them without a second thought. Each click got the hackers more access and information until they were able to access the campaign runners' accounts. The breach damaged the Clinton campaign multiple times before election day.

**THE TRUTH IS OUT THERE** As an increasing amount of our data is stored online, and our everyday lives unfurl in public, personal privacy and reputation come under threat in a number of new ways. And that means you need to update your strategies for staying safe. In earlier chapters, we've talked about broad-spectrum operations that seek to steal as much data as possible in the hopes that something will prove useful. In character attacks, the intention is often more personal and targeted, with the goal of damaging a specific person or group's reputation. These antisocial urges are nothing new, but technology makes it much easier to act on them. Back in the old days, people sought movie stars' racy photos through bribery or theft, but that was time consuming and expensive. And starting a nasty rumor? Sure, you could gossip, but how far would those lies really go? Today's troublemakers have more tools at their disposal that work anonymously—but you can still protect yourself and fight back. First, let's look at how they find your secrets.

**UP IN THE CLOUD** What we call "the cloud" is really just a bunch of computers sitting in data centers around the world talking to each other through global networks. These days, folks at a new start-up are likely to spend less time thinking about how many servers they need and more on how many cloud-computing resources they can use instead. The cloud provider takes care of

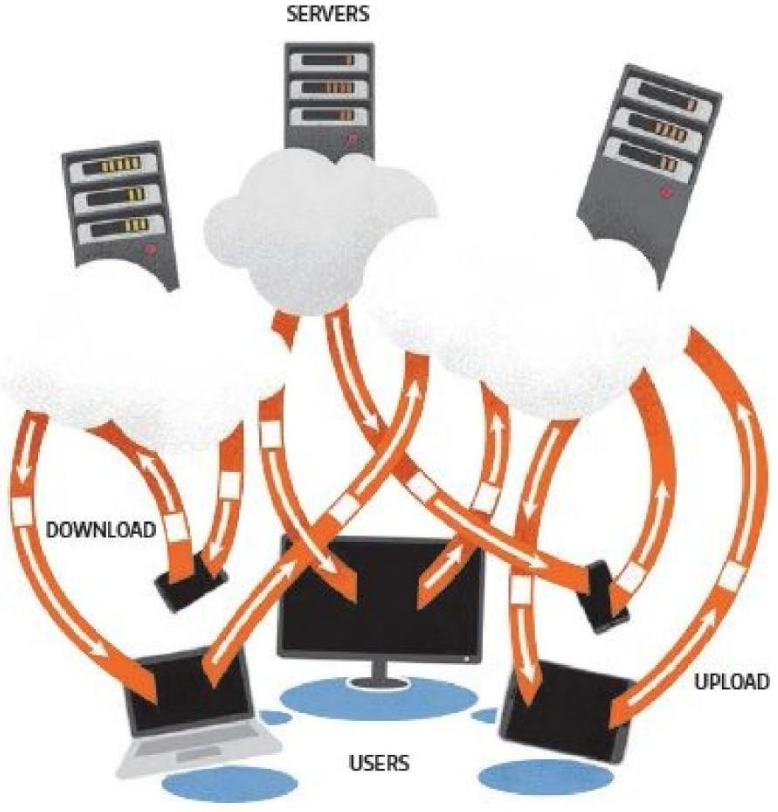
all the hardware, software, security, and physical assets through these data centers, and it also assumes much of the risk of owning lots of technology. By relying on such infrastructure giants as Microsoft Azure, Citrix, Oracle, Google, and others to provide the basic infrastructure, as well as tens of thousands of companies to handle all the details, that new business can start up faster and focus on what it does best, as opposed to managing expensive, space-hungry server farms. Sounds awesome, right?

**SAFETY CONCERNS** As more and more companies go completely cloud-based, new vulnerabilities arise. While cloud providers are very careful about protecting their own resources from being hacked and destroyed, they are less able to influence what happens once data shifts into areas controlled by their customers. So, for example, it would be extremely difficult to successfully attack Amazon and gain control of its servers. But once that data has been dispatched to, say, an individual user's Dropbox account, it gets a lot easier.

We don't believe for one second that Netflix, or Amazon Video, or Gmail, or Dropbox are inherently insecure. But they rely on users, and users make mistakes. In fact, most hacks begin when someone makes a mistake. Picture a real-life delivery system: No matter how well the U.S. Postal Service protects your deliveries, once the mail is in your mailbox, it's your responsibility. If it gets stolen, you can't blame the letter carrier.

Remember: Even though John Podesta's weak password (which was "Fluffy1," by the way) may have played a role in the spearphishing attack on the Clinton campaign's official email, the attack would never have succeeded without a whole bunch of people absentmindedly clicking on an unfamiliar link.

This chapter talks about how to avoid those mistakes, what can happen if you don't, and how to clean up any resulting mess.




**ANATOMY OF A CLOUD** What we loosely refer to as the cloud is an ever-evolving collection of hardware and software—the servers that make up the infrastructure and the platforms and applications that let end-users access it.

**REMEMBER TO TURN ON PRIVATE OR INCOGNITO BROWSING TO KEEP SITES FROM STORING COOKIES ON YOUR COMPUTER AND COLLECTING INFORMATION ABOUT YOUR VISIT WITHOUT YOUR**

## PERMISSION.

### ONLINE ATTACKS, REAL-WORLD IMPACT

**I'M A WOMAN WHO SPENT SEVENTEEN YEARS FIGHTING TO EARN MY TITLE OF VICE PRESIDENT IN THE OIL AND GAS INDUSTRY. IN A FEW SIMPLE KEYSTROKES, IT WAS ALL TAKEN AWAY FROM ME.**

I used to think the internet was fun: posting updates about my life on Facebook, creating a LinkedIn profile to network professionally, tweeting random thoughts, and taking pictures of the world around me to put on Instagram—nothing prolific, just little things. Friends gave me advice about how online profiles could help my career in a future in which people would read

about me online instead of talking to me in person. I trusted that the internet was a safe place to be.

Wow, how wrong I was!

I was thirty-seven years old when someone began to harass and cyberstalk me online. It began with false reports about me personally and professionally over numerous sites, from Twitter to Google+. The stalker created fake profiles of me on escort sites, harassed me on social media, and threatened me over the phone. Once, I was even sent a used condom in the mail, along with a note.

Then the cyberstalker raised the stakes and began to attack my friends, my family, and my company. When I didn't comply with the demands made of me, my tormentor posted bogus rip-off reports and reviews of the company I worked so hard to build. Every part of my life was targeted.

Until this began, I had never really understood the power of the internet or given very much thought on how I could navigate it safely.

As the cyberstalking intensified, as more information about me was posted in more places, I felt increasingly alone and that the rest of the world doubted me before even meeting me. I would walk into business meetings and be asked right away about intimate things no one would mention in the company of their own children, but because it was online, it was considered fair game.

People believe what they read online. Despite my efforts to set the record straight, I ended up losing contracts and ultimately my job. I couldn't trust anyone around me. I was under attack on all fronts. Some even exploited the situation to pressure me for money, blaming me for the impact my stalker had on their lives.

---

**"FOR THEM, IT WAS A SICK GAME; FOR ME, IT**

## WAS REALITY."

Two years of relentless psychological terrorism left me feeling hopeless, helpless, and powerless. I had been completely violated. I had nowhere to turn, since all of my attempts to involve the FBI and local police were met with the same answer: "We don't have the resources to help with a situation that doesn't involve murder." All I wanted was the answer to a simple question: "Why me?" Why would a stranger have so much hatred and feel the need to destroy a hardworking woman?

My now-husband and I had just started dating, and so it seemed likely that the attacks started out as an attempt by some unknown person to break us up. Instead, it forged us in fire. We were both broken to our cores, but we found our true love. We were married in the middle of this merciless attack, and now I have a teammate who is at my side until the end.

Two years on, the attacks still continue. I was advised that if I keep a low profile the attacker would eventually lose interest, but so far that has not been the case. So this year, I decided that I'd had enough. I decided to create a blog outlining all that had happened to me and the tools I found useful.

I am making sure my voice is heard. There are very few places to turn, and many are scams that cannot help you. My personal blog, www.stalkerexposed.com, explores in-depth the harsh realities of what can happen when someone wants to hurt you online. It is meant to serve as a reminder to everyone to take action and be safe online.

—Amanda Nickerson

## LESSON LEARNED

Amanda Nickerson believes that the best protection online is to have a good password and two-factor authentication (see page 29) on every site you can. As a proactive measure, bolster your legitimate online presence and keep it up to date. This is huge: The less there is online about you, the easier it is for trolls and stalkers to make your life difficult. Laws lag far behind modern tech, and many of the companies that host mean and outright made-up content on blogs don't even respond to complaints or demands. You'll end up having to hire lawyers to do takedowns.

Spend your energy on genuine and meaningful content about what you truly do instead of sinking time into fighting lies. Google rewards solid content with better rankings. It takes time, but your peace of mind and career will benefit from a concerted effort to curate a solid body of online content about yourself and your interests.

## SECURITY BASIC

**CHECK YOURSELF** You might not be able to stop someone from spreading fake stories about you, but you can make the harasser less likely to be taken seriously or even seen in search results.

Start by seeing what your online presence looks like right now. Using Chrome, open an incognito window or use duckduckgo.com and search for your name within double quotes ("Nick Selby"). The results will give you a sense of what a stranger Googling you would see. How does it look? Would you hire this person? Sell this individual a house? Go on a date with them?

Every month, check again to see what pops up. If your first check reveals nothing unusual, this exercise is just a formality. If, however, you discover that someone is trying to make you look bad, step up efforts to generate accurate content. Over time, the real you should rise in the rankings, while illegitimate sites fall away.

**WATCH OUT FOR TROLLS** Unfortunately, there's no shortage of women on the internet who still have to face random and sometimes extremely vicious harassment for little or no discernible reason or cause. While we fervently hope that in a few years our admonitions will seem as quaint and antiquated as a warning about spotting a dishonest footman, right now we'd be remiss not to touch on this unsavory topic. Women working in traditionally male-centric fields, such as gaming or technology, probably face the largest amount of abuse, but trolls can sometimes fixate on the strangest of things. One freelance journalist was testing blogging tools in order to set up a site; she posted a single goofy article on why she loves broccoli before abandoning the blog. Yet even this one article somehow touched a nerve: An unhinged stalker found that single post and made her life hell for more than a year. He made rape and death threats (the standard currency of the sexist troll), PhotoShopped her head onto pornographic images and mailed them to her employers and family, doxxed her, and even showed up outside her apartment to intimidate her in person. The threats never rose to a level that could get law enforcement involved, and it took her years to undo the damage. She still writes under a pseudonym and is very cautious about using any social media. Sound like a one-in-a-million crazy story? Not if you read Amanda Nickerson's case (see pages 50–51). In an even more unnerving case, best-selling writer Jessica Valenti recently dropped off all social media after the commenters who regularly threatened her with rape and murder started making the very same threats against the writer's five-year-old daughter.

**WHY THEY DO IT** Popular writer Lindy West was plagued by a troll who got under her skin by creating a Twitter account in the persona of her recently deceased father to pepper her with

insults and threats in his name. She wrote a fascinating piece about how painful this was—and unexpectedly got an email from the man behind the account. The resulting conversation (which you can hear on the popular podcast This American Life) was both illuminating and ultimately frustrating. He said that when he started harassing her, he was filled with self-loathing and was infuriated that she, a self-described fat woman, could be happy and successful. Why did this inspire him to torment and harass her? He had no good answer. It just seemed like the thing to do.

**DON'T BE DISCOURAGED** So, what's the takeaway for the average reader? Despite all of the above, the odds of this kind of random, sustained harassment are low. And, counterintuitively, while raising your profile may attract trolls, it will also give the kind of robust, impressive online presence that makes it more difficult for them to harm you. If you are harassed, report and block as necessary, and don't let them scare you away. In the unlikely event that such activity escalates, use the strategies outlined in chapter 11 to fight back.

**REPUTATION MATTERS** Modern commerce means doing business with all kinds of people you've never met but whom you still need to be able to trust. That's where online reputation comes in. Just as you have a reputation in your community, your school, your family, and with your friends, you also have one online that is based on your browsing history and activities.

The concept of online reputation was pioneered by the auction site eBay. As a global marketplace connecting buyers and sellers, the company had to offer tools to assure users that the strangers they are buying from are trustworthy.

If you use eBay, your reputation is based on whether you communicate well, pay on time, and send what was ordered... or

whether you tend to stiff buyers or raise hell over trivial matters. On Uber, your ratings are those assigned to you by drivers after each ride. Airbnb users rate your home online, and you, in turn, rate their performance as guests. Right now, reputation is not transferrable—eBay users don't have access to your Amazon rankings, and Uber drivers can't see what Lyft thinks of you—but that might well change in the future as the concept develops. Reputation is perhaps even more important to small businesses, and we'll discuss these factors in detail in chapter 7.

## SECURITY BASIC

**EYES AND EARS** In a 2016 photograph depicting Facebook CEO Mark Zuckerberg sitting at a desk, security folks noted that there was a piece of masking tape over the camera of his laptop. To those who wonder whether Zuck was being a little paranoid, he wasn't. In fact, closer examination showed that he had also disabled the microphone.

It was back in 2007 when I saw the first demonstration of a remote hack that stealthily turned on a user's camera and microphone, made a video, and sent it someplace, all without alerting the user. And the technology has really advanced since then.

To be safe, cover web-enabled cameras and microphones with masking or duct tape until you want to use them. This is what security nerds call a *positive security model*—that is, "deny by default, and allow by exception."

**WARDRIVING IS THE "SPORT" OF SCANNING FOR**

**UNSECURED, EASILY HACKED HOME NETWORKS. TO PROTECT YOURS, CHANGE THE DEFAULT PASSWORDS AND NAMES, AND ENCRYPT ALL TRAFFIC ON YOUR NETWORK.**

**SNATCHING SECRETS FROM THE AIR** Hackers love Wi-Fi, because these networks form one of the weakest points in an average user's online activity. And once they've breached your Wi-Fi, they can do a lot more than download Netflix on your bandwidth. A hacker can track and hijack the data you send and receive and use your connection to commit any number of crimes that could then be traced back to you. I've been on cases where the police literally kicked down a door, guns at the ready, to bust a major child pornography operation... only to find a very scared and confused older couple whose system had been hijacked. In that case, they were lucky the responding officers knew enough about cybercrime to suss out the situation. Not everyone is so lucky. Read on to learn some of the most common risks you face when going online wirelessly and how to defeat them.

**At Home** Loads of home networks are completely unsecured, which means they don't require a password for access. This exposes everything you transmit over that Wi-Fi connection to potential interception, and if that sounds like spy stuff, it shouldn't. You can learn how to harvest this bounty of information, if you are so inclined, with free software and instructional YouTube videos. Some networks are password protected, but the typical home user usually retains the default password that came with their wireless router. If this describes you, you may not be shocked to learn that there are entire

websites dedicated to cataloging the default passwords for nearly every router ever made. Secure your home network with a strong password and change it often to increase security.

**In Public** Hackers love coffee shops and hotel lobbies. Harried travelers and groggy commuters constantly use free public Wi-Fi connections with no thought for safety. If the networks are unsecured, they can be "sniffed" just like your home network. If they are secured, hackers may set up a second network that isn't with a deceptive name. For example, search for Wi-Fi on your phone the next time you're sitting in the lobby of a large hotel. You may well see a long list—some of them belonging to nearby residences or businesses. But in addition to the official Whitby Arms Inn, there may be networks named things like "Guest Rooms," "Hotel Network," or "Lobby Internet." They may even be cleverly named to be listed alphabetically above the real network and therefore easy to select. Always ask for the name of the business's official network, and if you have the choice of a password-protected option, take it. It might even be worth paying a modest usage fee for enhanced security.

**SURE SIGNS YOU'VE BEEN HACKED** Despite your best efforts at keeping your network locked down, there's always a chance that a black-hat hacker has broken into it. Luckily, there are plenty of ways to tell if that's happened. Here's a list of potential symptoms to diagnose a compromised network. (There are plenty of other possibilities out there, too; if something just doesn't feel right about your network, dig deeper and you might find something as the result of a hack.)

**Missed Connections** If your network is running slowly during an apparent quiet time, it could be the result of someone else using your bandwidth. Too many connections from too many users can clog a network, especially a smaller one. Check and see who's logged on, and make sure the devices belong to people you know and trust.

**A Lack of Control** Are you unable to log on to the network? That may indicate that the login or password has been changed; a sure sign someone else has gotten in and locked you out. Be sure you change your network's default password at the very least.

**Taking a Drive** If your machine's hard drive is running slower than usual, and you notice the activity light flashing a lot more than it should, look into the situation a little further: Your antivirus software could be running a scan—or someone could have broken in and used malware to scan your disk looking for interesting data to steal.

**Shields Down** Is your antivirus software disabled even though you swear it was set to start every time your machine boots up? Or even though you swear you just restarted it five minutes ago? A malware infection can often disable antivirus software.

**Unexpected Wares** Your browser window didn't have that toolbar the last time you used it. And those pop-up windows weren't authorized either. What program just started during bootup? You didn't set that up, did you? Check to see if any extra software has been installed that you didn't put in yourself. Chances are it's the result of a hack.

**No Shutdown** The system won't shut down when you tell it to? You could be prevented from doing so by a hacker who wants to stay on the system. (But you can always pull the plug.)

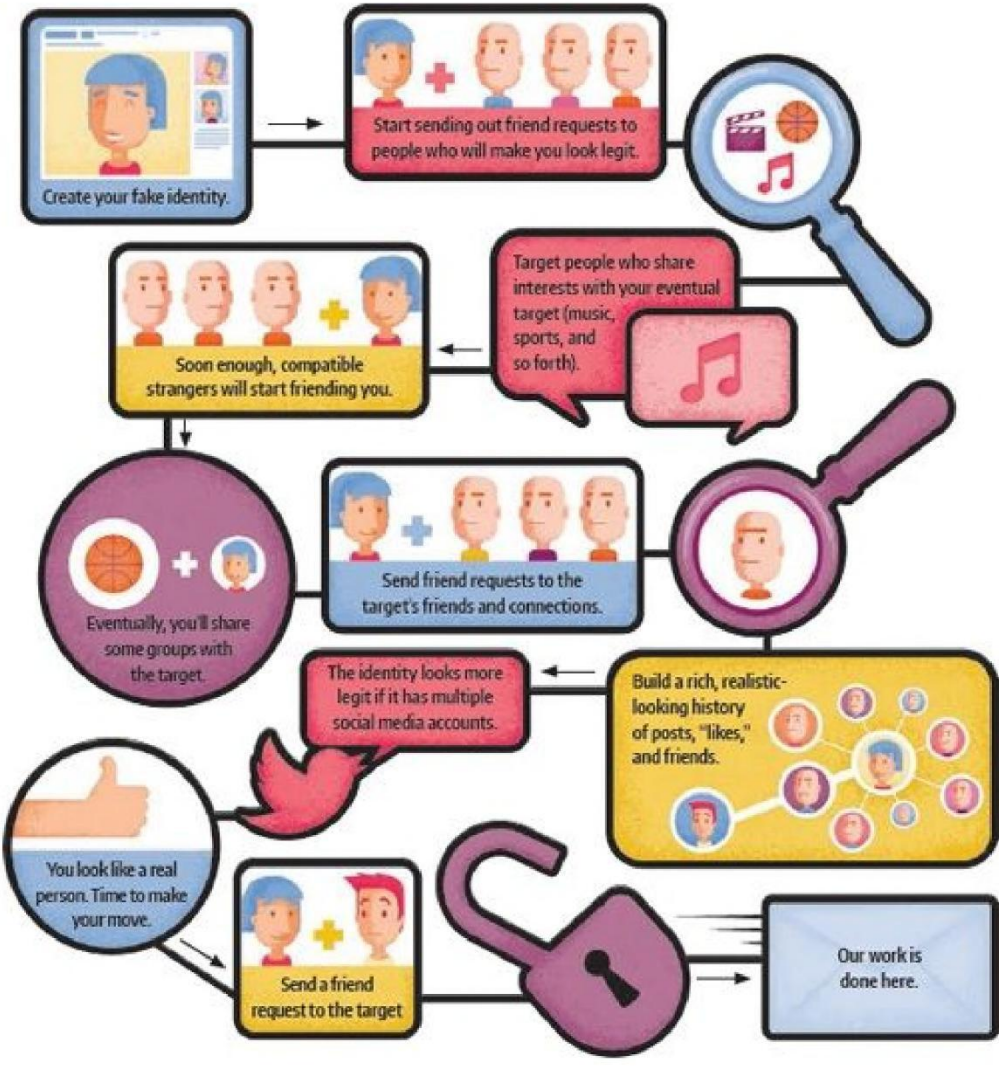
T/F

## WI-FI HACKING IS SO EASY, A KID CAN DO IT

**TRUE** You don't have to be trained in information technology work, or even be an adult, to know how to break in to someone else's system. All you really need is a computer with internet capability and a surprisingly short amount of time.

This was aptly proven during an ethical hacking demo in London in 2015, when seven-year-old Betsy Davies was shown a free YouTube video tutorial on how to fake a public Wi-Fi hot spot, then used it to get access to volunteers' computers—and in no more than eleven minutes.

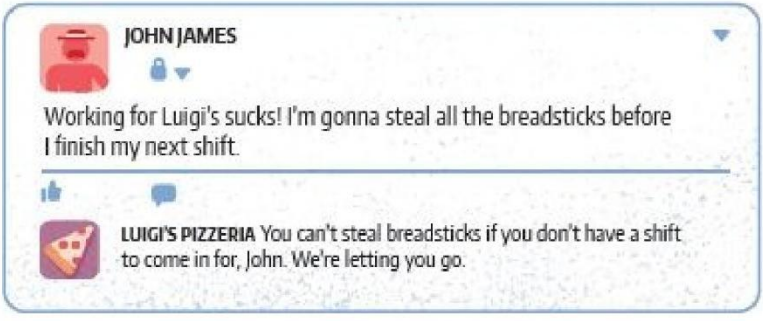
In short, anyone could be a hacker—even a kid on a laptop in a nearby library or coffee shop. And a skilled hacker with the means and the intent can do a lot more damage than a curious kid.




# A TANGLED WEB OF CONNECTIONS

I'M AN INVESTIGATOR WHO HAS SPENT MORE THAN A

**DECADE FIGHTING CYBERCRIME. IT'S COMMON FOR CRIMINALS AND CON MEN TO CONSTRUCT FAKE IDENTITIES AND COZY UP TO PERSONS OF INTEREST ONLINE. OF COURSE, THESE TECHNIQUES MIGHT ALSO BE USED BY COPS. HERE'S HOW A TYPICAL ONLINE "FRIEND" IS CONSTRUCTED.**




**THE PROBLEM OF OVERSHARING** Lots of parents think their kids share too much info online, and they're right; we'll talk more about that in the next chapter. But while adults may be less likely to suffer physical harm, bullying, or ridicule than their offspring, they're often just as guilty of sharing too much with their friends on social media—and the personal, financial, and career consequences can be significant. Consider just a few cases of grown-ups not practicing what they (hopefully) preach.

**Watch Me Fly** The CEO of a major gaming company spoke publicly about battling a series of hacks from an adversary called Lizard Squad. Sometime later, he posted online about a trip he was about to take. The hackers identified the specific flight he would be on and forced it to divert by tweeting a bomb threat to the airline. If the executive hadn't provided sufficient data for the hackers to figure out his travel details, his business trip wouldn't have been disrupted.

**Expensive Tweets** Michael Dell, the tech executive, pays millions of dollars a year for security to protect his family from potential kidnappers and other dangers. Finding that his teenage daughter had tweeted links to photos of a family trip, with details on where they'd be for the next few weeks, was probably a little frustrating. As evidenced by the swift disappearance of her Twitter account.

**Feeling Indiscreet** The Israeli army was forced to cancel a military operation after one of the soldiers taking part in it posted the location and date of their planned attack on Facebook.

**Busted!** A decorated member of the UK's Buckingham Palace Guard was sacked after ranting on Facebook, calling Kate Middleton, the Duchess of Cambridge, a variety of inappropriate names. Back in the more mundane world, internet meme sites are filled with screengrabs of Facebook sequences like this:

## CASE STUDY

**LET'S BE FRIENDS** In 2009, a male security researcher and white-hat hacker decided to see how easy it would be to get access to national security materials. He created LinkedIn and Facebook profiles for Robin Sage, a nonexistent female security expert supposedly working in "cyber threat analysis" at the Naval Network Warfare Command in Norfolk, Virginia, backed up by a fake work history and photos of an attractive young woman. In roughly eight weeks, the "Robin Sage Experiment" had access to emails, bank accounts, even classified military information from