

CHRISTOPHER HADNAGY
MICHELE FINCHER
FOREWORD BY ROBIN DREEKE

PHISHING DARK WATERS

The Offensive and Defensive
Sides of Malicious E-mails



WILEY

Table of Contents

[Introduction](#)

[Am I a Builder Yet?](#)

[Teaching People to Phish](#)

[What You Can Expect](#)

[Conventions Used in This Book](#)

[Summary](#)

[Notes](#)

[Chapter 1: An Introduction to the Wild World of Phishing](#)

[Phishing 101](#)

[How People Phish](#)

[Examples](#)

[Summary](#)

[Notes](#)

[Chapter 2: The Psychological Principles of Decision-Making](#)

[Decision-Making: Small Bits](#)

[It Seemed Like a Good Idea at the Time](#)

[How Phishers Bait the Hook](#)

[Introducing the Amygdala](#)

[Wash, Rinse, Repeat](#)

[Summary](#)

[Notes](#)

[Chapter 3: Influence and Manipulation](#)

[Why the Difference Matters to Us](#)

[How Do I Tell the Difference?](#)

[But the Bad Guys *Will* Use Manipulation ...](#)

[Lies, All Lies](#)

[P Is for Punishment](#)

[Principles of Influence](#)

[More Fun with Influence](#)

[Things to Know About Manipulation](#)

[Summary](#)

[Notes](#)

[Chapter 4: Lessons in Protection](#)

[Lesson One: Critical Thinking](#)

[Lesson Two: Learn to Hover](#)

[Lesson Three: URL Deciphering](#)

[Lesson Four: Analyzing E-mail Headers](#)

[Lesson Five: Sandboxing](#)

[The "Wall of Sheep," or a Net of Bad Ideas](#)

[Summary](#)

[Chapter 5: Plan Your Phishing Trip: Creating the Enterprise Phishing Program](#)

[The Basic Recipe](#)

[Developing the Program](#)

[Summary](#)

[Chapter 6: The Good, the Bad, and the Ugly: Policies and More](#)

[Oh, the Feels: Emotion and Policies](#)

[The Boss Is Exempt](#)

[I'll Just Patch One of the Holes](#)

[Phish Just Enough to Hate It](#)

[If You Spot a Phish, Call This Number](#)

[The Bad Guys Take Mondays Off](#)

[If You Can't See It, You Are Safe](#)

[The Lesson for Us All](#)

[Summary](#)

[Chapter 7: The Professional Phisher's Tackle Bag](#)

[Commercial Applications](#)

[Open Source Applications](#)

[Comparison Chart](#)

[Managed or Not](#)

[Summary](#)

[Chapter 8: Phish Like a Boss](#)

[Phishing the Deep End](#)

[Summary](#)

[Notes](#)

[End User License Agreement](#)

List of Illustrations

[Figure 1.1](#)

[Figure 1.2](#)

[Figure 1.3](#)

[Figure 1.4](#)

[Figure 1.5](#)

[Figure 1.6](#)

[Figure 1.7](#)

[Figure 1.8](#)

[Figure 1.9](#)

[Figure 1.10](#)

[Figure 1.11](#)

[Figure 1.12](#)

[Figure 1.13](#)

[Figure 1.14](#)

[Figure 1.15](#)

[Figure 1.16](#)

[Figure 1.17](#)

[Figure 1.18](#)

[Figure 1.19](#)

[Figure 1.20](#)

[Figure 1.21](#)

[Figure 2.1](#)

[Figure 2.2](#)

[Figure 2.3](#)

[Figure 2.4](#)

[Figure 2.5](#)

[Figure 2.6](#)

[Figure 2.7](#)

[Figure 2.8](#)

[Figure 2.9](#)

[Figure 3.1](#)

[Figure 3.2](#)

[Figure 3.3](#)

[Figure 3.4](#)

[Figure 3.5](#)

[Figure 3.6](#)

[Figure 3.7](#)

[Figure 4.1](#)

[Figure 4.2](#)

[Figure 4.3](#)

[Figure 4.4](#)

[Figure 4.5](#)

[Figure 4.6](#)

[Figure 4.7](#)

[Figure 4.8](#)

[Figure 4.9](#)

[Figure 5.1](#)

[Figure 5.2](#)

[Figure 5.3](#)

[Figure 7.1](#)

[Figure 7.2](#)

[Figure 7.3](#)

[Figure 7.4](#)

[Figure 7.5](#)

[Figure 7.6](#)

[Figure 7.7](#)

[Figure 7.8](#)

[Figure 7.9](#)

[Figure 7.10](#)

[Figure 7.11](#)

[Figure 7.12](#)

[Figure 7.13](#)

[Figure 7.14](#)

[Figure 7.15](#)

[Figure 7.16](#)

[Figure 7.17](#)

[Figure 7.18](#)

[Figure 7.19](#)

[Figure 7.20](#)

[Figure 7.21](#)

[Figure 7.22](#)

[Figure 7.23](#)

List of Tables

[Table 4.1](#)

[Table 4.2](#)

Introduction

“There was no such thing as a fair fight. All vulnerabilities must be exploited.”

—Cary Caffrey

Social engineering. Those two words have become a staple in most IT departments and, after the last couple years, in most of corporate America, too. One statistic states that more than 60 percent of all attacks had the “human factor” as either the crux of or a major piece of the attack. Analysis of almost all of the major hacking attacks from the past 12 months reveals that a large majority involved social engineering—a phishing e-mail, a spear phish, or a malicious phone call (vishing).

I have written two books analyzing and dissecting the psychology, physiology, and historical aspects of con men, scammers, and social engineers. And in doing so, I have found that one recent theme comes up, and that is e-mail. Since its beginning, e-mail has been used by scammers and social engineers to dupe people out of credentials, money, information, and much more.

In a recent report, the Radicati Group estimates that in 2014 there was an average of 191.4 billion e-mails sent each day. That equates to more than 69.8 trillion e-mails per year.^{[1](#)} Can you even imagine that number? That is 69,861,000,000,000—staggering, isn't it? Now try to swallow that more than 90 percent of e-mails are spam, according to the information on the Social-Engineer Infographic.^{[2](#)}

E-mail has become a part of life. We use it on our computers, our tablets, and our phones. In some groups of people that I've worked with, more than half the people

have told me that they get 100, 150, or 200 e-mails *per day!*

In 2014, the Radicati Group stated that there are 4.1 billion e-mail addresses in the world. Using that figure and a calculator, I discovered that the average is almost 50 e-mails per person per day, every day of the year. Because we know that not every single person in the world gets that many messages, it is not inconceivable to think that many of us receive 100, 150, or even 250 e-mails per day.

As people get more stressed, as workloads increase, and as the use of technology reaches an all-time high, the scam artists, con men, and social engineers know that e-mail is a great vector into our businesses and homes. Mix that with how easy it is to create fake e-mail accounts, spoof legitimate accounts, and fool people into taking actions that may not be in their best interests, and we can see why e-mail is quickly becoming the number-one vector for malicious attackers.

When we are not running social-engineering competitions at major conferences like DEF CON, and Michele is not fighting with students (real story, I swear), we travel the globe to work with some of the biggest and best companies on their security programs. Even companies that know what they are doing and have robust programs for security awareness and protection are still falling victim to the threat of phishing.

We wrote the pages of this book with that experience in mind. We asked ourselves, “How can we take the years of experience in working with some of the world's largest companies and help every company put a plan into action to make the most of phishing education?”

Am I a Builder Yet?

Michele and I started to develop a program that we implemented in a few places. The program is simple but powerful. It involves using the very tools that are used against us to empower us. We know that this concept is not something we invented. After all, there are more than a handful of companies right now selling “phishing services” to legitimate organizations. Many users of those products—large companies—have come to us and said things like, “We have been using this tool for a year, but our click ratios are still super high. What can we do?”

Before I answer that, let me tell you a story. I remember when I was buying my first home. My wife and I were super excited as the closing approached. (We were going to own a home!) So I did what all men who own a home do: I bought some more tools. I went to Home Depot and bought a beautiful set of cordless tools, a saw, a drill, a jigsaw, and some other miscellaneous tools.

I brought them into my house the first day and found the perfect spot on the shelves in the basement for that toolbox. There it sat for a year. Then all of a sudden I had to cut something. I was so excited; I finally got to use my new tools! I got the toolbox and pulled out the circular saw. I read all the instructions, including something like, “Ensure you are using the proper blade for the material you are cutting.”

I looked at the blade, thought, “Yep, looks sharp,” and cut my board. It worked. I still had all my limbs and appendages, the board was cut, and the saw didn't blow up. This process continued for a couple hours when all of a sudden the saw started jamming; it stopped cutting. I charged the batteries and did the finger-touch test to the blade and thought, “Ouch, still sharp.” Frustrated, I determined the tool was at fault. “Stupid saw; must be defective.”

Then a friend came over to help me out. He took one look at the saw and said, “Um, dude, why are you cutting 2×4s with a fine-tooth blade?”

“A what-toothed what?” I replied.

My friend shook his head, and then he gave me an education on blades.

Why do I tell you this humiliating, emasculating story other than to point out my utter lack of manliness? To prove this point: Owning tools does *not* make you a builder!

Phishing tools are no different than construction tools. Just buying the tool doesn't make you secure, and it doesn't make you able to educate others on the phishing problem.

Teaching People to Phish

So, back to the program Michele and I were developing: We started to analyze phishing and security awareness programs and discovered—as many other serious security professionals have determined—that many of them were useless.

No, security awareness is not useless. I'm not so naïve and silly to say that we don't need awareness. But the style and method of awareness training just wasn't working.

Seriously, raise your hand right now if you ever paid attention all the way through a 30- or 60-minute DVD presentation on security awareness. Okay—the one guy in the back—you can put your hand down. But as I suspected, barely a hand is raised.

People tune out training if it's not interactive and *quick*. Marketers know this; they tell us to make websites interesting, fun, interactive, and to the point. Why should education be anything less?

We started to come up with a plan to make the phishing portion of our clients' security awareness interactive, interesting, and, most of all, not too lengthy. That is why this book had to be written; we wanted to answer a few questions:

- How serious is phishing?
- What psychological principles play a part in phishing?
- Can phishing really be used as a *successful* part of your security awareness education?
- If so, how can a company implement that?
- Can any size business create a serious phishing education program?

We sat down and outlined a book on phishing, defined our program, and formalized our methodology. We then gave a lot of thought to whether we wanted to release this to the public; after all, it took us years of work to develop our method. After we started to see how it was helping so many of our clients, we decided to write the book. On first approach, though, it seemed like a phishing book wasn't of much interest to many—at least not until the events of 2014, when phishing dominated the front pages again and again during real hacking events. Phishing is being used in attacks every day; phishing service providers are popping up every month; and companies all over the globe are jumping on the bandwagon to start phishing education programs.

What You Can Expect

Michele and I hope that this book will help you on your quest to protect yourself and your company against

malicious phishers. We want to take you on the journey we went through in getting ready to write this book.

Chapter 1 starts with the basics. It explains what phishing is and why it is used, and we included a lot of examples of the most current and effective phish.

Chapter 2 delves into the *why* of phishing. Why do those phish work? What is the psychology behind them that makes phishing so effective?

Chapter 3 takes a look at just one area—influence—and explains how that principle is used by malicious phishers.

Chapter 4 is all about protection. Now that the first three chapters have covered the bases of what phishing is, it's time to start discussing how you can protect yourself from it. We give tips for both civilians and corporations, as well as analyze some of the worst suggestions we have heard.

Chapter 5 gets into how you can create a corporate phishing program to help secure your folks.

But how do you tie all this information into corporate policies? I know, I know; the word *policy* is like a four-letter word in these books. But we have to discuss it, and the brief but important Chapter 6 is where we do that.

This book wouldn't be complete without looking at some of the most current tools on the market and how they work to complement the program being set up. Chapter 7 covers those tools.

Chapter 8 concludes the book by rounding off all the principles and discussion with some clear-cut rules of making this program work.

Conventions Used in This Book

To help you get the most from the text and keep track of what's happening, we used some conventions throughout the book.

Special formatting in the text represents the following things:

- We *highlight* new terms and important words when we introduce them.
- We show URLs within the text like so: www.social-engineer.org/.

Note

Notes indicate notes, tips, hints, tricks, or asides to the current discussion.

Summary

The idea behind this book is to dissect what a phish is, why it works, and the principles behind it. We want to fully expose all the flaws of phishing so you can understand how to defend against it.

In my last book, *Unmasking the Social Engineer*, I told a story about a friend who is a master swordsman. He learned his skill by learning all about swords—how to use them and how they work—and then choosing the best partner to help him learn how to fight with them. That story applies here, too. After you learn all about identifying phish, become familiar with the available tools, and learn how to choose a good sparring partner, you can then begin to create a program that will hone your skills and help you and your employees, family, and friends stay secure.

Before we can get that deep into the ring, we need to start with some light weights, including learning some key elements such as “What is phishing?” and “What are some examples of it?”

Read on to find out the answers to these questions.

Notes

1. Sara Radicati, PhD, “Email Statistics Report, 2014–2018,” April 2014, <http://www.radicati.com/wp/wp-content/uploads/2014/01/Email-Statistics-Report-2014-2018-Executive-Summary.pdf>.
2. Social-Engineer Infographic, April 28, 2014, <http://www.social-engineer.org/resources/social-engineering-infographic/>.

Chapter 1

An Introduction to the Wild World of Phishing

Lana: Do you think this is some kind of a trap?

*Archer: What? No, I don't think it's a trap!
Although I never do ...and it very often is.*

—Archer, Season 4 Episode 13

Because we're going to be spending some time together, I feel I should start our relationship with an honest self-disclosure. Although I consider myself to be a reasonably smart person, I have made an inestimable number of stupid mistakes. Many of these started with me yelling, “Hey, watch this!” or thinking to myself, “I wonder what would happen if *<insert dangerous/stupid situation here>*.” But most often, my mistakes have come not from yelling challenges or thinking about possibilities but from *not thinking at all*. This absence of thinking typically has led to only one conclusion—taking an impulsive action.

Scammers, criminals, and con men have clearly met me in a past life, because this is one of the key aspects that make them successful. Phishing in its various forms has become a high-profile attack vector used by these folks because it's a relatively easy way to reach others and get them to act without thinking.

NOTE

One more thing before this train really gets rolling. You may notice that when I refer to the bad guy, I use the pronoun “he.” (See? I even said bad “guy.”) I'm not sexist, nor am I saying all scammers are male. It's just simpler than improperly using “they” or saying “he or she” just to be inoffensive to someone, and it avoids adding a layer of complexity that's off the point. So “he” does bad stuff. But a bad guy can be anyone.

Phishing 101

Let's start with some basic information. What is *phishing*? We define it as the practice of sending e-mails that appear to be from reputable sources with the goal of influencing or gaining personal information. That is a long way of saying that phishing involves sneaky e-mails from bad people. It combines both social engineering and technical trickery. It could involve an attachment within the e-mail that loads malware (malicious software) onto your computer. It could also be a link to an illegitimate website. These websites can trick you into downloading malware or handing over your personal information. Furthermore, *spear phishing* is a very targeted form of this activity. Attackers take the time to conduct research into targets and create messages that are personal and relevant. Because of this, spear phish can be very hard to detect and even harder to defend against.

Anyone on this planet with an e-mail address has likely received a phish, and on the basis of the reported numbers, many have clicked. Let's be very clear about something. Clicking doesn't make you stupid. It's a mistake that happens when you don't take the time to think things

through or simply don't have the information to make a good decision. (Me driving from Biloxi, MS, to Tucson, AZ, in one shot, now *that* was stupid.)

It's probably safe to say that there are common targets and common attackers. Phishers' motives tend to be pretty typical: money or information (which usually leads to money). If you are one of the many who has received an e-mail urging you to assist a dethroned prince in moving his inheritance, you've been a part of the numbers game. Very few of us are fabulously wealthy. But when a phisher gets a bunch of regular people to help the prince by donating a small "transfer fee" to assist the flow of funds (often requested in these scams), it starts to add up. Or, if an e-mail from "your bank" gets you to hand over your personal information, it could have drastic financial consequences if your identity is stolen.

Other probable targets are the worker bees at any company. Although they alone may not have much information, mistakenly handing over login information can get an attacker into the company network. This can be the endgame if the rewards are big enough, or it might just be a way to escalate an attack to other opportunities.

Other than regular people, there are clearly high-value targets that include folks located somewhere in the direct food chain of large corporations and governments. The higher people are in the organization, the more likely they are to become targets of spear phish because of the time and effort it takes to get to them and the resultant payoff. This is when the consequences can become dire at the level of entire economies as opposed to individuals.

If you move beyond the common criminal and the common motive of quick money, the rationale and the attackers can get big and scary pretty quickly. At one end of that, there might be people interested in the public embarrassment of

a large organization for political or personal beliefs. For example, the Syrian Electronic Army (SEA) has been cited in a number of recent cases in which phishing e-mails led to the compromise of several media organizations, including the Associated Press (AP),¹ CNN,² and Forbes,³ just to name a few. Clearly, there have been financial consequences; for instance, the hack of the AP Twitter account caused a 143-point drop in the Dow (see [Figure 1.1](#)). No small potatoes, but what about the public loss of reputation for a major media outlet? We could debate all day which consequence was actually more costly. On a positive note, however, it did make all of us reconsider whether social media is the best way to get reliable, breaking news.



[Figure 1.1](#) Hacked AP tweet

Going even deeper, we get into cyber espionage at the corporate and/or nation-state level. Now we're talking about trade secrets, global economies, and national security. At this point, the consequences and fallout become clear to even the most uninformed citizen. A current story rocking international news alleges that Chinese military attackers have breached five major U.S. companies and a labor union.⁴ The companies are part of the nuclear and solar power and steel manufacturing industries. For the first time in history, the United States has brought charges

of cyber espionage against another country.⁵ All of this was initiated by some simple e-mails.

I guess this is a long way of saying that phishing should matter to everyone, not just security nerds. Cyber espionage might not be something you think about every day, but I'll bet your bank account and credit score are something you do give thought to. My mother *still* hasn't figured out how to check her voicemail on her cell phone (true story!), but she's definitely aware that she should never open an e-mail from someone she doesn't know. Your mom should follow that rule, too.

Now you know the what, the who, and the why; let's talk about the how.

How People Phish

Identifying a suspect e-mail would probably be pretty easy if the sender was "Gimme Your Money." But one of the simplest ways that con men take advantage of us is by the use of *e-mail spoofing*, which is when the information in the "From" section of the e-mail is falsified, making it appear as if it is coming from someone you know or another legitimate source (such as your cable company). Chris and I outline some simple steps in [Chapter 4](#) that might help you identify whether the sender is legitimate. In the meantime, it's simply good to know that thinking an e-mail is safe just because you know the sender isn't always a sure bet.

Another technique that scammers use to add credibility to their story is the use of *website cloning*. In this technique, scammers copy legitimate websites to fool you into entering personally identifiable information (PII) or login credentials. These fake sites can also be used to directly attack your computer. An example that Chris personally experienced is the fake [Amazon.com](#) website. This is a great

example for a couple of reasons. First, it's a very common scam because so many of us have ordered from [Amazon.com](https://www.amazon.com). We've seen the company's website and e-mails so many times that we probably don't take a very close look at either. Second, it's good enough that even someone very experienced in the sneaky tactics used by scammers almost fell victim to it.

Chris has been phishing our clients for years (with their permission, of course). He's sent hundreds of thousands of phish and knows how they're put together and why they work. But last year, he received an e-mail informing him that access to his [Amazon.com](https://www.amazon.com) account was going to be blocked. This e-mail happened to coincide with preparations for our annual contest at DEF CON. Now, there's never a time that Chris isn't busy, but the month or so prior to DEF CON is basically all nine circles of Dante's Hell at the same time, in his office. I don't know what he actually thought or said at the time he received the fake [Amazon.com](https://www.amazon.com) e-mail, but you probably know where this story is going. [Figure 1.2](#) shows the very e-mail he received.

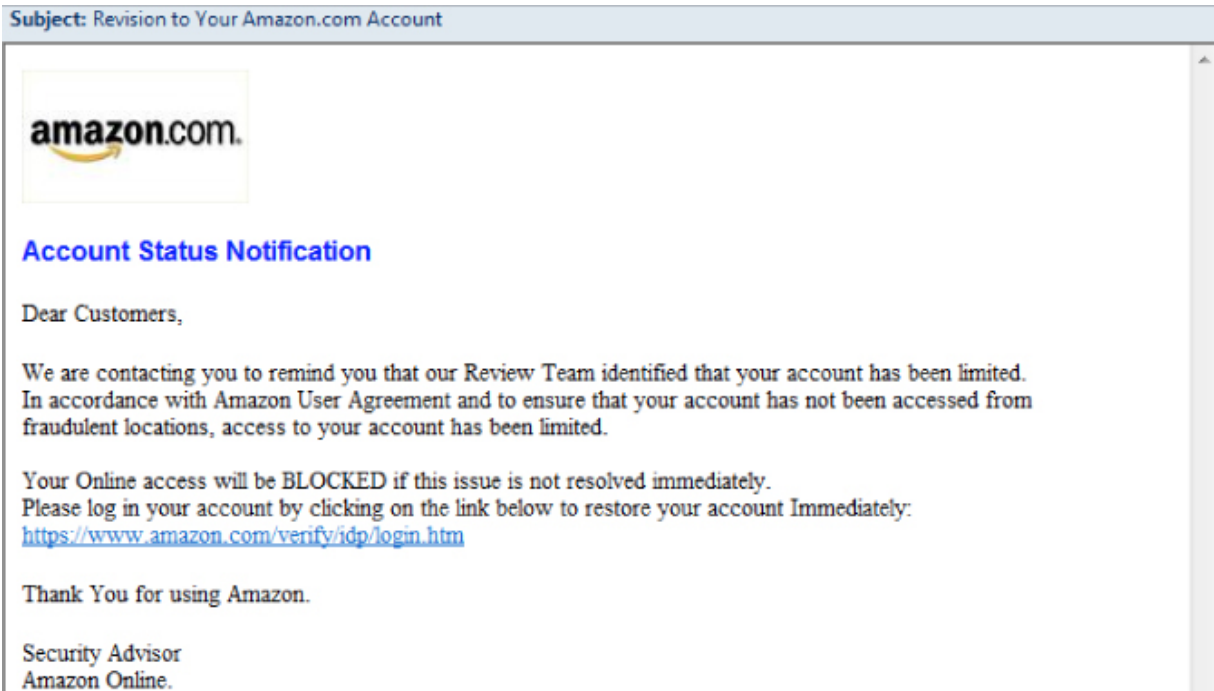


Figure 1.2 The infamous [Amazon.com](https://www.amazon.com) phishing e-mail

If you read this e-mail closely, you will notice that the language isn't quite up to par, and there are anomalies, such as random capitalization. These characteristics are common hallmarks of phish, as many senders aren't native English speakers. The key here is that the quality of the e-mail is more than good enough to pass a quick inspection by a recipient with his hair on fire.

Chris clicked the link and ended up on what looked like the [Amazon.com](https://www.amazon.com) website, as shown in [Figure 1.3](#). Even a close visual inspection wouldn't have been revealed it as fake because the site had been cloned.

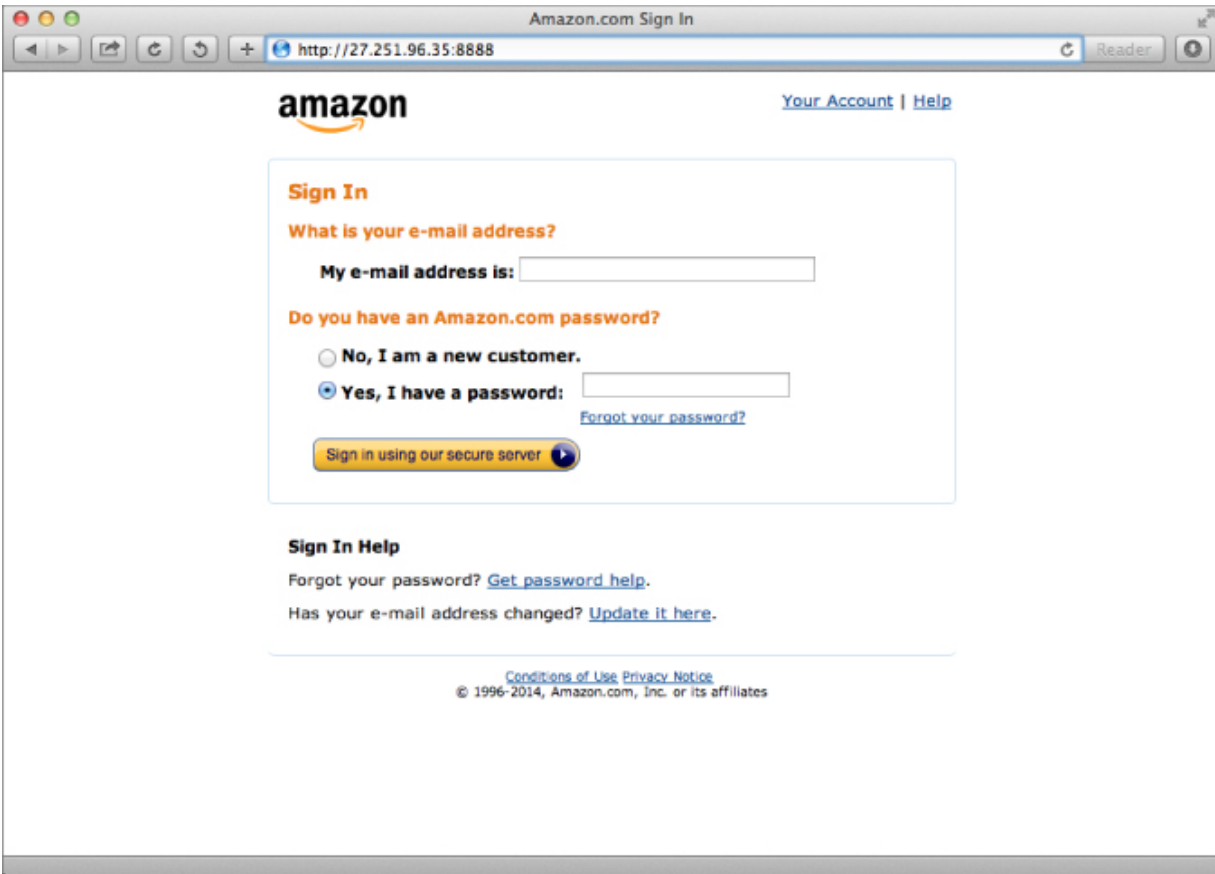


Figure 1.3 Fake [Amazon.com](#) website

At this point, Chris's years of training kicked in. He looked at the website URL (address) and realized it wasn't legitimate. If he had entered his login credentials as he was asked to, his account containing his PII and his credit card information would have been hijacked. This almost worked because the website itself was an exact duplicate of the real thing, and the e-mail came at a time when Chris was busy, tired, and distracted—all things that can prevent critical thinking. (We'll talk more about this in [Chapter 4](#).) The bottom line here is that website cloning is a very convincing way of getting people to believe the phish is real.

One final trick that scammers use is to follow up phishing e-mails with a phone call. This is also known as *vishing* (for voice phishing) or phone phishing. Vishing has many

malicious goals, ranging from adding truthfulness and credibility to an e-mail all the way to directly requesting confidential information. This technique emphasizes the idea that you should be closely protecting your PII. I grew up in an era in which people regularly had their Social Security and telephone numbers printed on their checks, right under their addresses, which basically announced, “Please steal my identity, Mr. Criminal!” Imagine how convincing it would be if you received an e-mail directly followed by a phone call from “your bank” that urged you to click the link, go to a website, and update your account information.

A real example occurred recently at the corporate level. It was dubbed “Francophoning” because the targets were primarily companies based in France.⁶ The attack was well planned and executed. An administrative assistant received an e-mail regarding an invoice, which was followed by a phone call by someone claiming to be a vice president within the company. He asked the assistant to process the invoice immediately. She clicked the e-mail link, which led to a file that loaded malware. This malware enabled attackers to take over her computer and steal information. This example is interesting because so many factors are in play—for example, the use of authority and gender differences in compliance—but the main point here is that any story becomes more convincing if you hear it from more than one source.

Examples

I'm not sure about you, but both Chris and I learn best by example. This section covers some high-profile compromises that started with phish and some of the most prevalently used phish on the market today. We also discuss why they work so well.

First of all, this section would be incomplete if we didn't mention the Anti-Phishing Working Group (APWG—www.apwg.org). We could fill pages about how amazing these folks are, but the thing to know is that the APWG is a global coalition of security enthusiasts who study, define, and report on how phishing is working around the world.

According to the APWG's report dated August 2014, phishing numbers continue to be staggering. In the second quarter of calendar year 2014, there were 128,378 unique phishing sites reported and 171,801 unique e-mail reports received by APWG from consumers.⁷ This was the second-highest number of phishing sites detected in one quarter since the APWG started tracking these statistics. Payment services and the financial industry were the most targeted sectors, accounting for 60 percent of the total, but within that, there was also a new trend in which online payment and crypto-currency users were targeted at an increased rate.

Now that you've seen the bird's-eye view of the numbers, it's time to examine some specifics.

High-Profile Breaches

Target Corporation is probably one of the highest-profile breaches to date. It has affected close to 110 million consumers—an estimated 40 million credit cards and 70 million people with stolen PII; with those numbers, you might have been one of them.⁸ The interesting thing about this story, however, is that it appears as though the attack wasn't specifically aimed at Target.⁹ This is a prime example of attack escalation. Target became a victim of opportunity after the real breach. The initial victim in this case was an HVAC vendor for Target that had network credentials. A person at the HVAC company received a phishing e-mail and clicked a link that loaded malware,

which in turn stole login credentials from the contractor. The contractor network had connections to the Target network for things such as billing and contract submission. Not all of the attack details are known, but after attackers had access to snoop around, they eventually found entry into Target's corporate servers and compromised the payment system.

Although the final hit to consumers is still to be determined, the Target breach has already cost more than \$200M for financial institutions to reissue compromised credit cards—and that's before taking into account any charges for fraud, which consumers aren't liable for. All in all, this was a dramatic and expensive lesson in the dangers of phishing.

Another notable breach that you may not even remember involved RSA. At this point, any mention of RSA probably relates to the encryption controversy it experienced in connection to the National Security Agency starting in late 2013. That story was so big that it practically overshadows the corporate breach the company experienced in 2011.^{[10](#)} Unlike the opportunistic Target attack, this one appears to have been a very deliberate action taken against RSA employees. It was apparently the result of a malicious Excel spreadsheet attachment to an e-mail sent to low-level RSA users (see [Figure 1.4](#)).

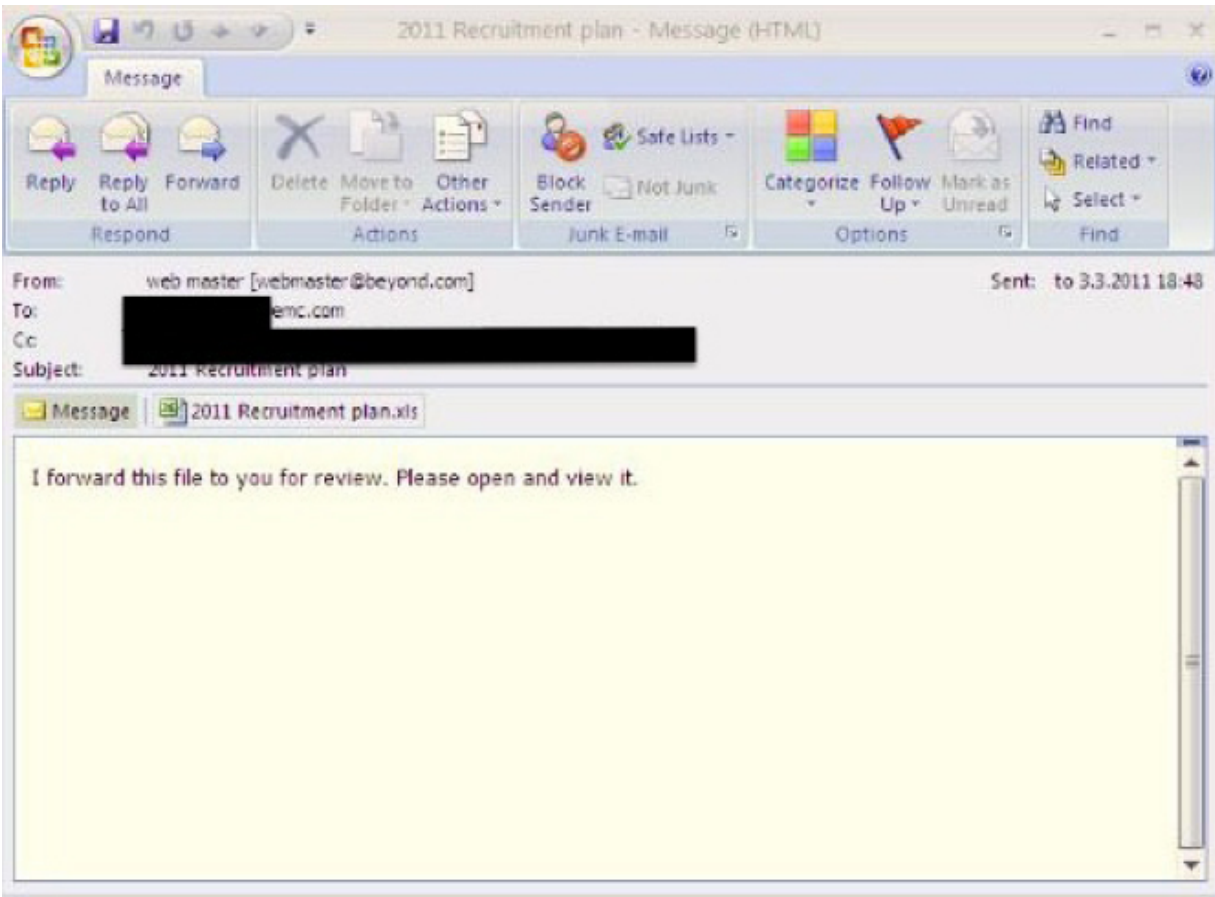


Figure 1.4 RSA phish

RSA's spam filters reportedly caught the e-mails, sending them to users' Junk folders. The interesting point here is that humans overrode technical controls that worked the way they should have. At least one recipient opened the e-mail and clicked the attachment. This gave attackers entry into the internal network and enabled them to eventually steal information related to some of RSA's products. It was reported that in the quarter that followed the breach, parent company EMC spent \$66M on cleanup costs, such as transaction monitoring and encryption token replacements.

One more product-based company breach worth noting involved Coca-Cola in 2009.¹¹ This case originated as a very targeted spear phish directed at Coca-Cola executives