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. 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 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 e-mail, but you probably know where this story is going. Figure 1-2 shows the very e-mail he received.

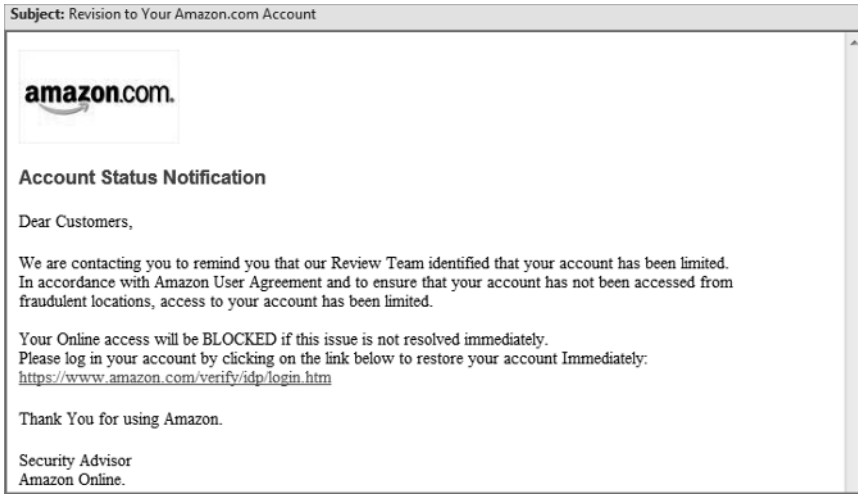


Figure 1-2: The infamous Amazon.com phishing e-mail

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 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.

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.

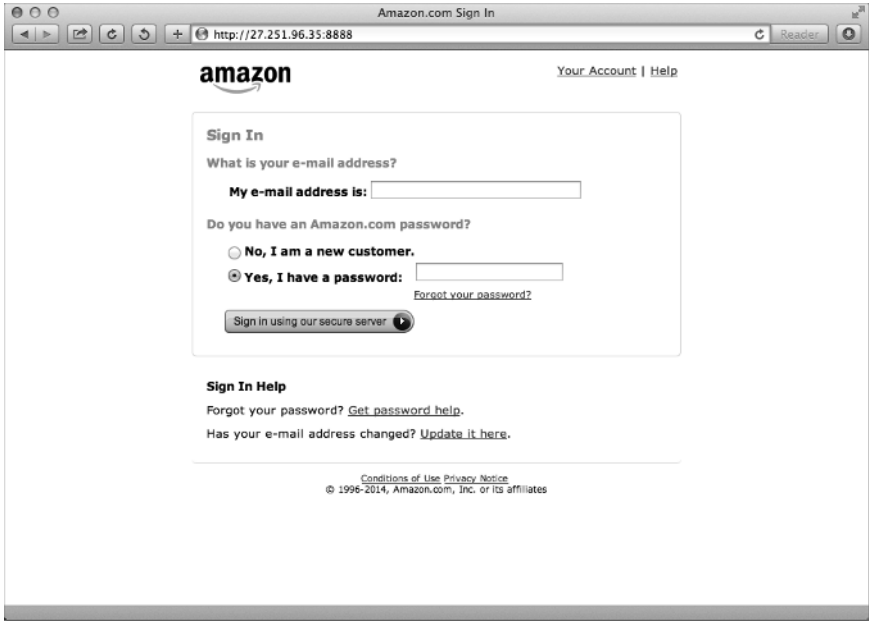


Figure 1-3: Fake Amazon.com website

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).

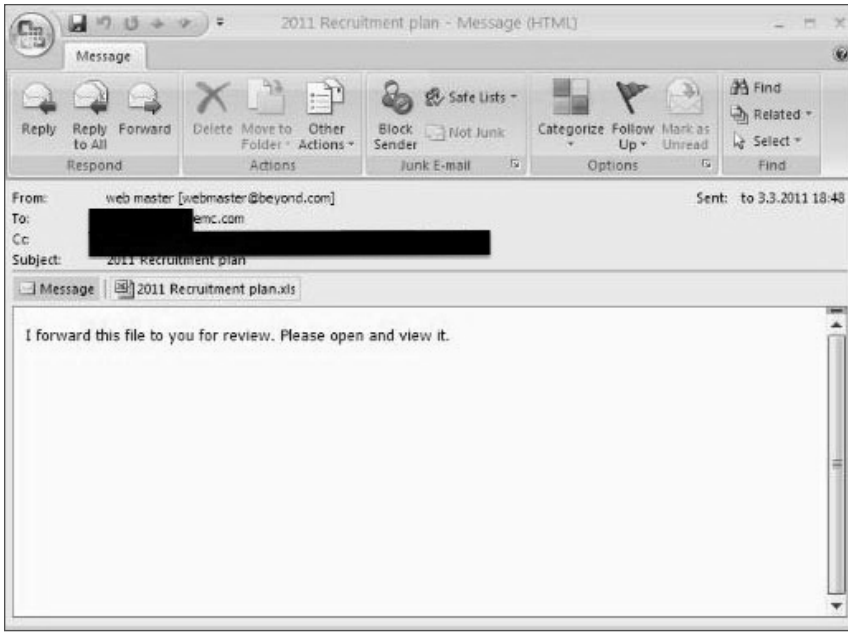


Figure 1-4: RSA phish

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 with the subject line "Save power is save money! (from CEO)." The e-mail subject line is pretty bad, to be sure, but consider a couple of things: First, the e-mail appeared to come from an exec in the legal department at Coca-Cola. Second, at the time of the attack the company was promoting an energy-saving campaign. (The attackers really had done their homework.) The exec opened the e-mail and clicked the link, which was supposed to lead to more information about the energy program. Instead, he ended up loading a bunch of malware, including a key logger that tracked everything he typed in the weeks to come. This breach allowed the Chinese attackers to gain access to the internal corporate network and mine data for weeks before being discovered.

This breach occurred in February 2009, and Coca-Cola wasn't aware of it until the FBI informed the company in March. By then a great deal of sensitive data had been stolen. This was days before Coca-Cola's $2.4B attempt to purchase a Chinese soft drink manufacturer, which ultimately failed. It would have been the largest acquisition of a Chinese company by a foreign entity to date. There are conflicting reports as to why the acquisition failed, but at least one security organization claims it was due to critical information regarding strategy and pricing being leaked to the opposite side, which deprived Coca-Cola of the ability to negotiate the deal.

As mentioned earlier, the hack of the AP was impressive based solely on the sheer impact that one tweet had on the stock market.[12] The way the attackers got in, however, was a simple spear phish that was sent to select AP staffers from what appeared to be a colleague (see Figure 1-5).

Although this e-mail is pretty vague, consider that it came from a "known" source and appeared to point to a legitimate page on *The Washington Post* site. Victims who clicked the link in the message were sent to a spoofed website that collected their login credentials. There's speculation that the spoofed site allowed victims to authenticate with their Twitter credentials, which led to the feed compromise.

Corporations are clearly as vulnerable to phishing as regular people are despite all of their technical controls and security policies. So what about phish that hit a little closer to home? The following section describes common examples that you may have seen.

Sent: Tue 4/23/2013 12:12 PM
From: [An AP staffer]
Subject: News

Hello,

Please read the following article, it's very important :

http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/23/

[A different AP staffer]
Associated Press
San Diego
mobile [removed]

Figure 1-5: Associated Press spear phish

Phish in Their Natural Habitat

We would be doing the topic of phishing a disservice if we didn't start with the *Nigerian 419* scam. Also known as the *advance-fee fraud*, this con is apparently more than 200 years old in practice (as you can imagine, it took a lot longer to get scammed over snail mail, but it still happened). It gets its most modern name because of Nigeria's notoriety as supposedly being a large source of these scams. The number 419 refers to the Nigerian criminal code that addresses fraud.

You have probably seen a number of variations of this scam. For example, a rich prince has been deposed and needs your help in transferring his vast wealth, or a dying man is trying to make up for being generally unpleasant and needs your help in disbursing funds to charity organizations. Whatever the cover story, a few components are consistent:

- The amount of money in question is vast.
- They are trusting *you*, a complete stranger, to transfer, disburse, or hold the money.
- You get a cut for your trouble, but you need to do one of the following:
  - Provide your bank account information so they can transfer the money
  - Assist them by paying transfer fees, mostly due to some sort of precarious political or personal situation

Figure 1-6 shows a real example of one e-mail I recently received. Okay, so this one came from a guy in Ghana, but you get the general idea.

[redacted] May 5, 2014 2:57 PM

To: johnson.adiyah@yahoo.com
Opportunity

From: Mr. Johnson Adiyah
Director of Projects
Department of Minerals & Energy
Ghana

Hello,

I write to ask for your indulgence in re-profiling funds up to the tune of Eight Million Five Hundred Thousand United States Dollars (US$8.5 Million) which I will want to keep safely overseas under your supervision. In other words, I would like you to receive the said funds my our behalf. The Funds were derived over time from a project awarded to a foreign firm by my Department, and presently the actual contract cost have been paid to the original project executors, leaving the balance in the tune of the said amount which we have in principle obtained approval to remit overseas.

Kindly pardon the use of a medium informal as this for reaching out to you to make a request of such a great importance. Currently, I work as the Director of Projects at the Department of Minerals & Energy here in Ghana.

This endeavor has a minimal risk factor on your part provided you treat it with the utmost discretion. You are advised to reach me through email for further clarifications.

Email: johnson.adiyah@yahoo.com

I kindly wait to hear from you.

Yours sincerely,

Mr. Johnson Adiyah

Figure 1-6: Michele's Nigerian 419 phish

This is probably a pretty obvious scam to the vast majority of people, but what are some specifics that told me this wasn't a legitimate offer from African royalty?

- I don't know any African royalty—or anyone from the Department of Minerals and Energy in Ghana, for that matter. I don't even know anyone named Johnson Adiyah.
- There's no reason Johnson Adiyah would know me, either. Well, he apparently doesn't, because he didn't actually greet me by name. A deal this big and he doesn't even *know my name*?!?
- Although I appreciate spontaneity, this offer is really, really out of the blue.
- They are entrusting me (as opposed to a bank or a trust or even a law firm) to handle $8.5 million. Just roll that around in your head for a minute. Now, I like to think I'm a generally trustworthy person, but do you know *how much cake and crab* I could buy with $8.5M?

- Finally, although I believe the sender used a spell-checker, this person's use of language is a bit off; it sounds like English is not Johnson Adiyah's native language—which would be okay if I actually knew a Johnson Adiyah in Ghana.

The Nigerian 419 scam really is at the beginner level of phishing scams. It's pretty obviously a fake and easy to detect. You would think that we'd catch on to this particular scam after 200 years. However, it's alive and well and still ensnaring somebody, probably even as you are reading this. Why does it still work?

- **Greed:** It's the first reason and also the most base. Most people will never see large sums of money such as that offered in the 419 phish, and that alone can keep people from thinking straight. There's always a chance that the story is true, right? Well, not really. But if you can talk yourself into believing you have a real shot at winning the lottery, it's probably not that much further to convince yourself that a stranger really would let you hold his money.
- **Lack of education:** We talk a lot more about this factor at various points later in this book, but there is a population of folks out there (which, until recently, included my mom) who have no idea that bad people might try to steal their identity or money through e-mail.
- **Plain gullibility:** There are people in the world that place their full trust in the word of others. It would be wonderful if we really lived in a world where that kind of trust didn't put us in an unsafe position.

Other than someone offering you vast riches, there are a number of very common themes that bad guys like to use. Some of these are good enough to at least give you pause.

Financial Themes

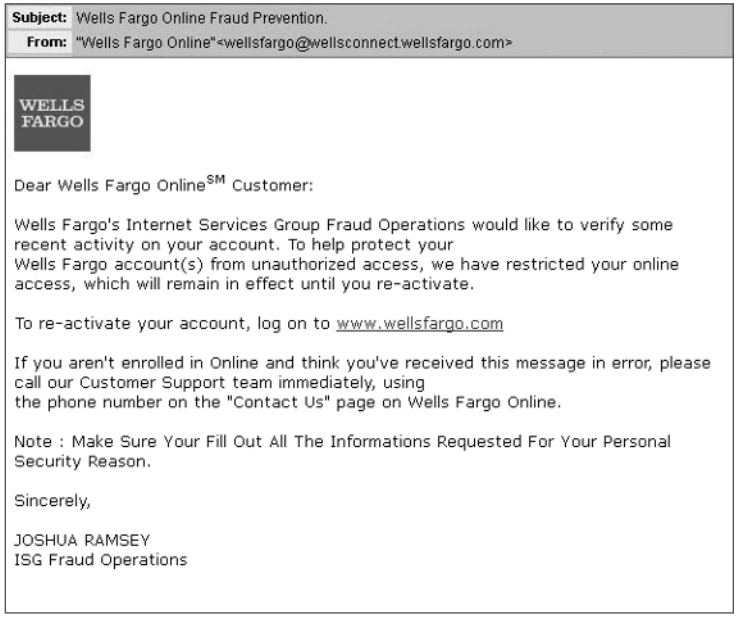
Financial themes are a big favorite of phishers. Most of us put our money somewhere, move it around, and pay taxes, so receiving a notice from a financial institution is typically enough to make us at least open the e-mail. The varieties of phish are endless, and they usually require you to validate your identity by submitting your account details through an online form. Some of the most common financial phish include the following:

- There have been a number of invalid login attempts on your account.
- Your bank has upgraded its online security.
- You are overdue on a loan or paying taxes.

Figures 1-7 through 1-10 show examples of phish in the wild. Most of these attempts are significantly better and more sophisticated than the Nigerian phish; they might contain logos and images, which makes them look much more legitimate. Let's classify these as the intermediate level of phishing scams.

Despite the greater finesse involved in these phish, there are still some details that will help you identify the fakers:

- Greetings still typically are vague; shouldn't your bank know your name? "Valued Customer" doesn't count.
- Spelling, grammar, and capitalization, although better, can still be a little off.
- Links to online validation forms indicate the web address doesn't really belong to the alleged sender.
- Use of urgent language ("Please respond immediately or access to your account will be blocked").



Subject: Wells Fargo Online Fraud Prevention.
From: "Wells Fargo Online"<wellsfargo@wellsconnect.wellsfargo.com>

WELLS FARGO

Dear Wells Fargo Online℠ Customer:

Wells Fargo's Internet Services Group Fraud Operations would like to verify some recent activity on your account. To help protect your
Wells Fargo account(s) from unauthorized access, we have restricted your online access, which will remain in effect until you re-activate.

To re-activate your account, log on to www.wellsfargo.com

If you aren't enrolled in Online and think you've received this message in error, please call our Customer Support team immediately, using
the phone number on the "Contact Us" page on Wells Fargo Online.

Note : Make Sure Your Fill Out All The Informations Requested For Your Personal Security Reason.

Sincerely,

JOSHUA RAMSEY
ISG Fraud Operations

Figure 1-7: Wells Fargo phish example

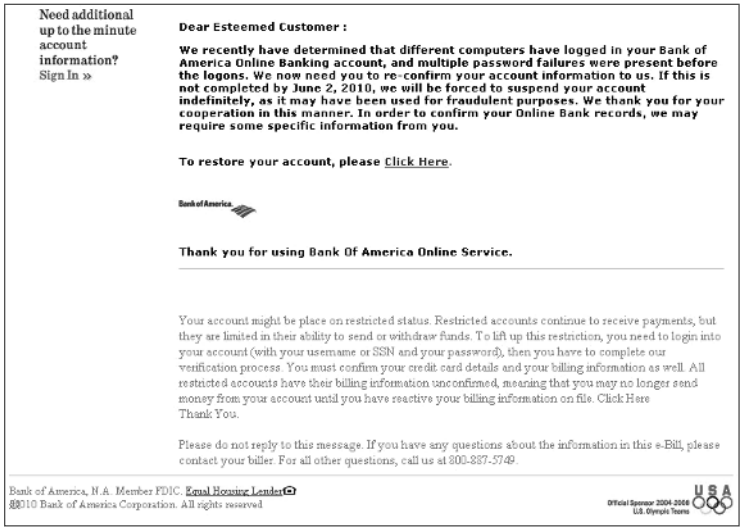


Figure 1-8: Bank of America phish example

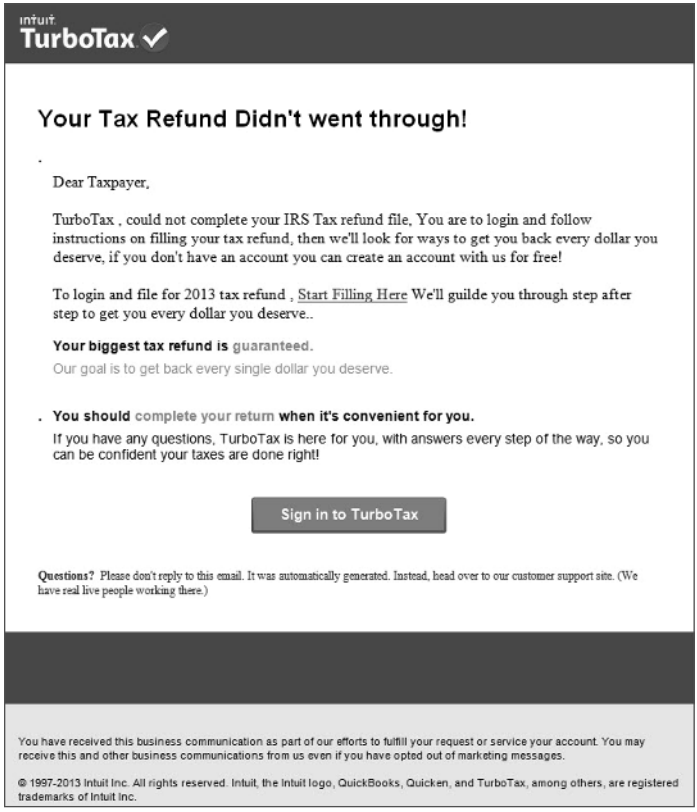


Figure 1-9: Tax filing phish example

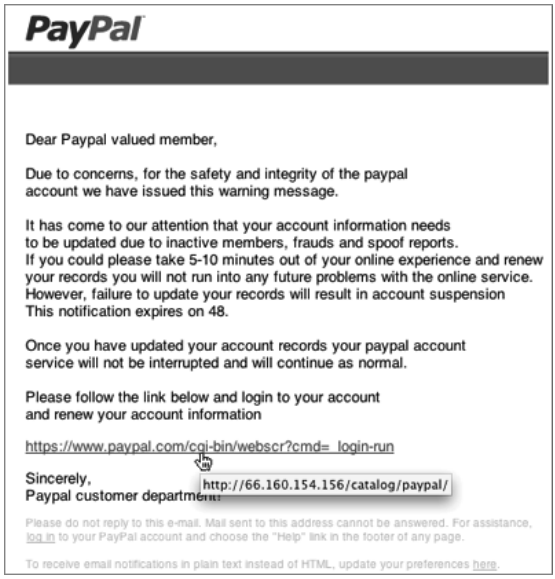


Figure 1-10: PayPal phish example

These e-mails coerce action mainly through a certain level of fear or apprehension. Anything that threatens access to your money is scary. In fact, most of the examples throughout this section have a great many things in common, especially in the way they get people to act:

- **Use of authority:** This is a principle of influence that is covered in depth in Chapter 3, but basically people are social creatures and we all respond to authority in one form or another.
- **Time constraints:** Oh, no! It says that access to your account expires in 48 hours! This kind of language really increases the level of anxiety. Because of our survival instinct, anything that limits access to a resource feels threatening.
- **Possible compromise:** It's truly frightening to think that your bank has detected what could be someone poking around in your accounts. The only person who should be swimming around in my gold pieces is me. And possibly Smaug.

Social Media Threats

Another common theme you may have seen is phishing through the use of social media. Come on—the point of social media is to be,

well, social. So getting an e-mail through one of the services notifying you of friend requests or asking you to check out a link makes perfect sense. In general, these types of e-mail are at about the same level of difficulty as, and can be identified as illegitimate by the same details as, the financial services phish. In my opinion, though, some of these are easier to fall for because if you participate in social media, getting an invitation of some sort is common and, more important, desirable. In addition these phish might not set off the same alarms that an unsolicited bank e-mail would so you may be less guarded in your response.

Like the financial services phish, these types of e-mails will sometimes use fear to encourage behavior, such as the one shown in Figure 1-11.


Subject: GooglePartnerService sent you a message: The Youtube Team
From: YouTube Service <service@youtube.com>
Date: 12:19 AM
To: [redacted]

YouTube Broadcast Yourself™

GooglePartnerService has sent you a message:

The Youtube Team

The Youtube Team
YouTube Broadcast Yourself™

Warning [redacted]

According to our records, you have been flagged for the following:

Hate Speech/Bullying
Spam/Flooding of other YouTube channels
Massive Advertising
Explicit Copyright Infringement

Your account also appears to be phished and/or flagged by other users with the following IP addresses:

72.55.191.6:3128
80.227.1.100:8080
119.70.40.101:8080
216.194.70.3:8118
61.166.68.69:80
194.44.170.81:3128

We have reviewed your account and notice that your account seems to be in good standing. Therefore, we reports made to your account, and notice that your account has been flagged and/or reported multiple time owner of this account and to verify your current account status. Please prov... more

You can reply to this message by visiting your inbox.

Figure 1-11: YouTube phish example

Fear is a great universal motivator, but losing access to a social media account is more of an inconvenience than a critical event (well, for *most* of us, anyway). However, the social media pretext also gives attackers a

couple of alternatives to the use of fear through encouraging participation and connection. These attacks also prey on a sense of obligation. Social media sites grow through the connections that are made. They make participation fun and make you a part of a tribe. Phishing attacks play on those same themes. A lot of people click because they don't want to hurt others' feelings by not accepting a friend request, or they don't want to seem rude by not responding—even to people they don't know. (See Figures 1-12 and 1-13.)

Figure 1-12: Facebook phish example

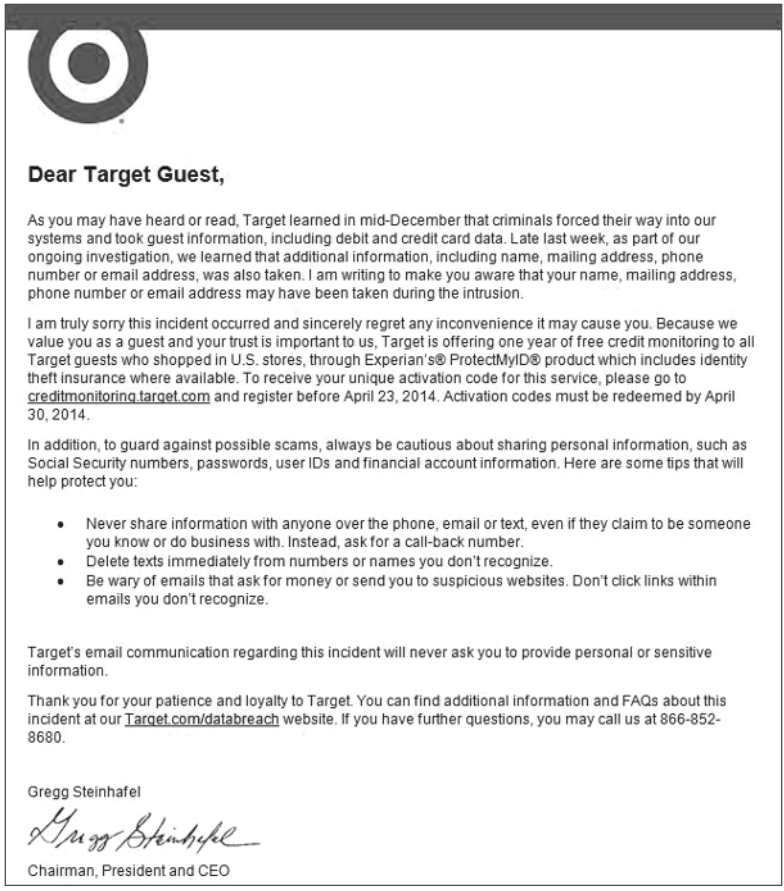
NOTE **You know, I had a sort of virtual relationship when I was a kid. She was a pen pal. I distinctly remember that it didn't have the power or immediacy that virtual relationships seem to have for many people today. The phenomenon of social media is still a really interesting thing to me. It's created a quick and fairly effortless way for people to connect far beyond their typical social and professional circles. Unfortunately, it also makes folks who are interested in meeting people and developing their networks particularly vulnerable to this type of phishing. In this case, it's good to be someone content to live under a rock. I literally have 34 legitimate invitations sitting in one of my accounts right now. I should probably learn to be a little less laissez-faire, or people will think I don't want friends.**

Figure 1-13: LinkedIn phish example

High-Profile Event Scams

A final category of phish in the wild that you may have seen is particularly heinous. Scammers send phish directly after a high-profile event, such as a natural disaster, plane crash, or terrorist attack—basically anything that receives massive media attention and therefore is in the forefront of most people's minds. They take advantage of our natural reactions of fear, curiosity, and compassion. These examples are still mostly at a very intermediate level when examined with a critical eye. They contain obvious indicators that they're not legitimate. That said, some people are vulnerable to falling for these types of phish simply based on their emotional response to the situation. And really, what's the best way to keep someone from thinking straight? Incite strong emotion. Chapter 2 talks about an interesting phenomenon called "amygdala hijacking."

Within 24 hours of Target announcing its breach, scammers started exploiting people's anxieties about the status of their personal and financial information. There were at least 12 different scams identified, one of which was identical to Target's e-mail to customers explaining the event and offering free credit monitoring.[13] As shown in Figure 1-14, this phish would have been difficult for anyone to catch. Because the text was an exact copy of what was sent by Target, you would have had to check the sender e-mail or the links. One more thing that made this one really tricky: The real e-mail from Target came from sender `TargetNews@target.bfi0.com`, which looked dodgy to everyone. Confusion and fear reigned, and the situation was definitely abused by the bad guys.



Dear Target Guest,

As you may have heard or read, Target learned in mid-December that criminals forced their way into our systems and took guest information, including debit and credit card data. Late last week, as part of our ongoing investigation, we learned that additional information, including name, mailing address, phone number or email address, was also taken. I am writing to make you aware that your name, mailing address, phone number or email address may have been taken during the intrusion.

I am truly sorry this incident occurred and sincerely regret any inconvenience it may cause you. Because we value you as a guest and your trust is important to us, Target is offering one year of free credit monitoring to all Target guests who shopped in U.S. stores, through Experian's® ProtectMyID® product which includes identity theft insurance where available. To receive your unique activation code for this service, please go to creditmonitoring.target.com and register before April 23, 2014. Activation codes must be redeemed by April 30, 2014.

In addition, to guard against possible scams, always be cautious about sharing personal information, such as Social Security numbers, passwords, user IDs and financial account information. Here are some tips that will help protect you:

- Never share information with anyone over the phone, email or text, even if they claim to be someone you know or do business with. Instead, ask for a call-back number.
- Delete texts immediately from numbers or names you don't recognize.
- Be wary of emails that ask for money or send you to suspicious websites. Don't click links within emails you don't recognize.

Target's email communication regarding this incident will never ask you to provide personal or sensitive information.

Thank you for your patience and loyalty to Target. You can find additional information and FAQs about this incident at our Target.com/databreach website. If you have further questions, you may call us at 866-852-8680.

Gregg Steinhafel

Chairman, President and CEO

Figure 1-14: Real or phish?

Obviously people with Target accounts were most vulnerable to these scams. Target is such a massive retail outlet, though, that the breach was enough to raise everyone's blood pressure a point or two. Is there anyone out there who hasn't shopped at Target at least once in his or her lifetime?

Chris and I are here to educate, not judge, but the post-disaster variants of high-profile event scams are undeniably some of the most deplorable. Instead of trying to intimidate (which is bad enough), these threats exploit your connection to others. Within hours of the Boston Marathon bombings, scammers were already hitting inboxes.[14] Many were very simple e-mails that provided a link to supposed videos of the explosions. Taking advantage of people's natural curiosity, these links led to websites that downloaded malware. A variant used both authority and curiosity through spoofing an e-mail from CNN (see Figure 1-15).

The worst, of course, are those phish that take advantage of people's desire to help others. Within hours of any tragic event, scammers are sending

out pleas for help. Figure 1-16 shows one of the e-mails that circulated after an earthquake and subsequent tsunami hit Japan in 2011. Reports indicated that scams were seen three hours after the initial earthquake.

Figure 1-15: Boston Marathon variant

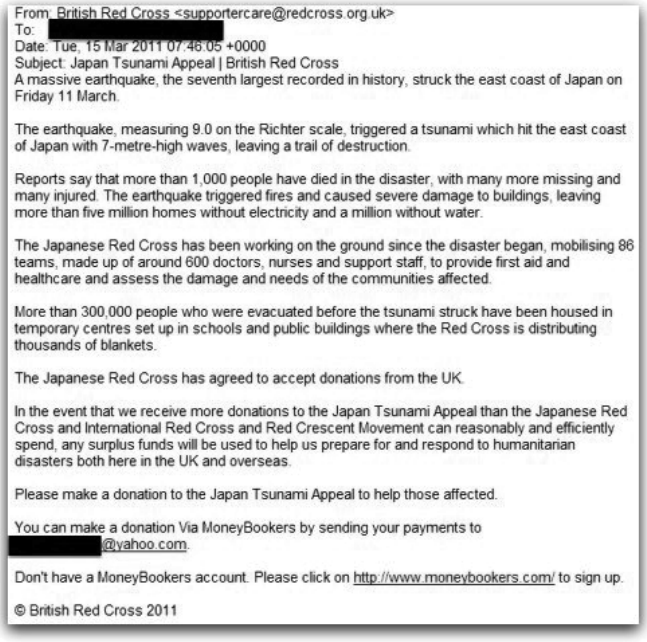


Figure 1-16: Japanese tsunami phish

The example in Figure 1-16 is pretty easy to identify as a phish because the Red Cross accepts donations directly on its website as opposed to taking wired funds through a service like MoneyBookers to an `@yahoo` e-mail address. But again, after such a tragic and high-profile event, a lot of people were eager to help. Simple phish aside, perpetrators of many of these disaster scams reinforce their stories with phone calls and even door-to-door solicitation, which increases their appearance of legitimacy.

Phish in a Barrel

To summarize this section, phish in the wild come in a variety of types, but some common themes are

- Nigerian 419 (advance fee or identity theft variants)
- Financial/payment services
- Social media
- High-profile event exploitation

The list actually goes on and on and can include any entity that can communicate online (think eBay, Netflix, software updates, and USPS), but you get the drift. Most of these phish can be classified at a beginner to intermediate level of sophistication and have a lot of commonalities. For instance they use the following to coerce action:

- Greed
- Fear
- Respect for authority
- Desire to connect
- Curiosity
- Compassion

Most phish at these difficulty levels have indicators that can help you identify them as not legitimate. However, the characteristics really start to become less obvious when you get to more advanced levels:

- Vague greeting/sign off
- Unknown/suspicious sender
- Links to unknown/suspicious web addresses
- Typos and grammar, spelling, and punctuation errors
- Implausible pretexts (especially with 419 scams)
- Urgent language

Phish with Bigger Teeth

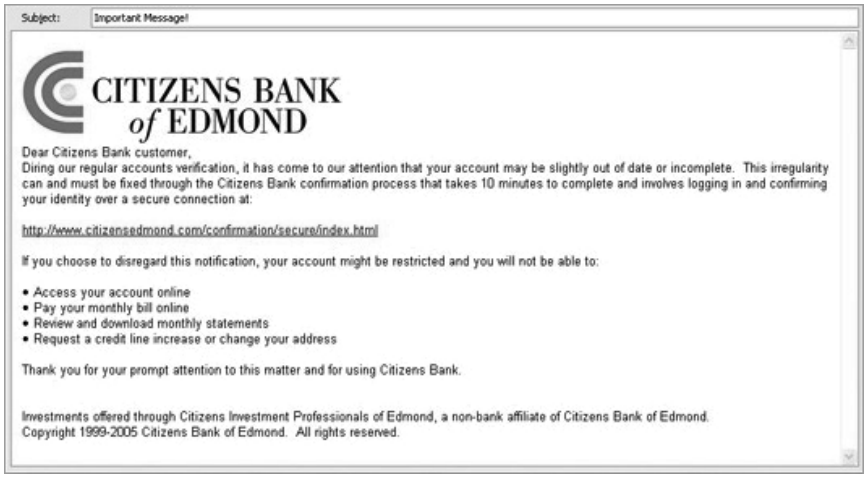
Do you feel like you've taken a drink from the fire hose yet? The deviousness and ingenuity that people use to steal from others is truly overwhelming. Even worse, the previous examples just touch on the most basic phish. There are additional variations that add complexity to a whole new (and depressing) level.

Chris and I started categorizing levels of difficulty in order to help our clients understand what they're seeing and also to track clients' progress in identifying progressively harder phish. We'll get into specific difficulty levels and their descriptions in Chapter 6.

Intermediate Phish

The examples you've already seen are mostly at the beginner and intermediate levels, but some of the examples thus far would definitely fall on the high-intermediate end of the spectrum. For example, the Target letter was an exact copy of the real thing except for links to bad websites. So let's do a little deep dive into the trickier ones and break them down a little bit.

Our first example is another bank phish, as shown in Figure 1-17.


Subject: Important Message!

CITIZENS BANK of EDMOND

Dear Citizens Bank customer,
Diring our regular accounts verification, it has come to our attention that your account may be slightly out of date or incomplete. This irregularity can and must be fixed through the Citizens Bank confirmation process that takes 10 minutes to complete and involves logging in and confirming your identity over a secure connection at:

http://www.citizensedmond.com/confirmation/secure/index.html

If you choose to disregard this notification, your account might be restricted and you will not be able to:

- Access your account online
- Pay your monthly bill online
- Review and download monthly statements
- Request a credit line increase or change your address

Thank you for your prompt attention to this matter and for using Citizens Bank.

Investments offered through Citizens Investment Professionals of Edmond, a non-bank affiliate of Citizens Bank of Edmond.
Copyright 1999-2005 Citizens Bank of Edmond. All rights reserved.

Figure 1-17: Intermediate bank phish

Let's talk about what these guys did "right." What are the things that might have made people click the link in the e-mail?

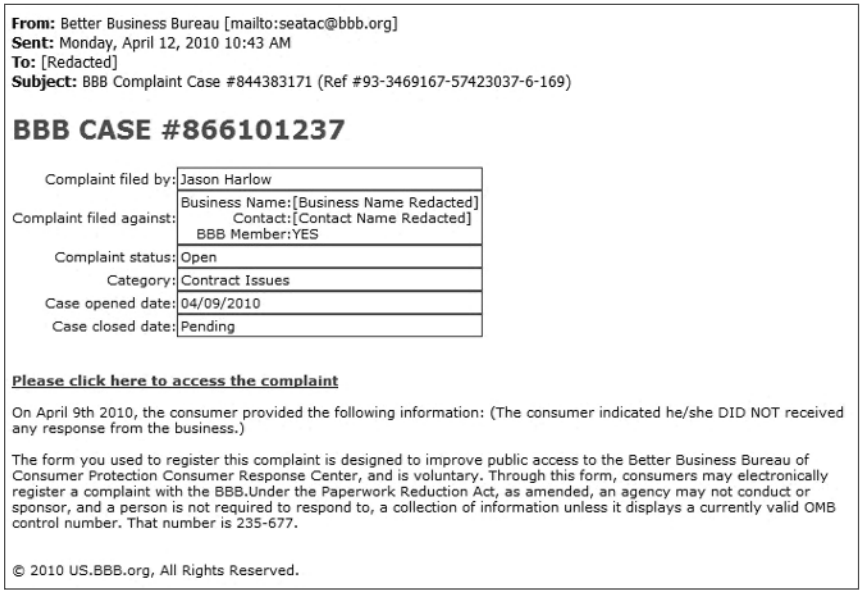
- **Bank logo**: You probably noticed this earlier, but many of the more advanced phish insert real logos and graphics, which makes them look more legitimate. Because we've gotten accustomed to seeing branding when companies communicate with us, including logos is one way to disguise a malicious message and keep us from really taking a close look.
- **Use of fear/anxiety**: The e-mail states that if you don't take action, your access to your money might be limited.
- **Use of urgent language**: The message doesn't go so far as to say your action has to take place in a set amount of time, but you're certainly encouraged to take prompt action.

After everything we've talked about thus far, I'm hoping the phish shown in Figure 1-17 was pretty easy for you to identify. Did you catch the tells?

- Nonpersonalized greeting.
- No identification of sender.
- Grammar oddities, including unlikely subject line.
- Link redirect. If you investigate the link, chances are that it doesn't go to real the bank website (for example, instead of going to `www.citizensedmond.com`, it actually goes to `www.unknownandlikelyillegitimateperson.com`).

WARNING **By investigate, we mean to hover your cursor over the link so you can see the web address. Never click, and never copy/paste the URL into a browser unless you're a security pro and have a Kevlar-fortified computer.**

On the surface, the example shown in Figure 1-18 is fairly similar to the previous bank e-mail, but there are a couple of things to point out that might make this a little more difficult to identify as a scam. Take a look and see what you think.



From: Better Business Bureau [mailto:seatac@bbb.org]
Sent: Monday, April 12, 2010 10:43 AM
To: [Redacted]
Subject: BBB Complaint Case #844383171 (Ref #93-3469167-57423037-6-169)

BBB CASE #866101237

Complaint filed by:	Jason Harlow
Complaint filed against:	Business Name:[Business Name Redacted] Contact:[Contact Name Redacted] BBB Member:YES
Complaint status:	Open
Category:	Contract Issues
Case opened date:	04/09/2010
Case closed date:	Pending

Please click here to access the complaint

On April 9th 2010, the consumer provided the following information: (The consumer indicated he/she DID NOT received any response from the business.)

The form you used to register this complaint is designed to improve public access to the Better Business Bureau of Consumer Protection Consumer Response Center, and is voluntary. Through this form, consumers may electronically register a complaint with the BBB.Under the Paperwork Reduction Act, as amended, an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number. That number is 235-677.

Figure 1-18: Intermediate BBB phish

If you looked closely, you probably caught at least a couple of the following details that make the phish in Figure 1-18 a better-than-average attempt:

- **Better personalization:** This was clearly sent to an individual and referenced that person's business. Although there was no use of imaging or logo, the Better Business Bureau is a well-known organization.
- **Better use of fear/anxiety:** This e-mail is a complaint, comes from the BBB, and specifically mentions contract issues *and* the fact that the business has not responded to the complainant. These are all enough to raise alarms with a business owner.
- **Use of authority:** There are all kinds of reference numbers, case numbers, OMB numbers—it all looks really official.
- **E-mail address:** The sender's e-mail address looks feasible; it appears to come from the `@bbb.org` domain.

Fortunately, there are still some weaknesses with this e-mail; did you spot them?

- The case number in the subject line does not match the case number in the body of the e-mail.
- No identification of sender. Sure, it's coming from the BBB, but you would think there would be a person assigned to be your point of contact.

- Again, if we *investigated* the link to access the complaint, we would find it doesn't go to a BBB-owned domain.
- There are still minor grammar errors.
- There's no such thing as the Better Business Bureau of Consumer Protection Consumer Response Center. I looked it up.

Advanced Phish

Okay, it's time to look at something a little harder to identify. The example shown in Figure 1-19 is an advanced-level phish. Unlike the LinkedIn e-mail shown in Figure 1-13, this one is trickier to identify as a scam. I suspect it is a clone of e-mails you would get that invite you to connect, along the lines of the Target e-mail shown in Figure 1-14.

Figure 1-19: Advanced LinkedIn phish

Why would this e-mail work?

- It's coming from a "real" person. He has a LinkedIn account, so he must be real, right?
- It's social media, so you expect to get invitations from people you don't know.
- It's branded and identical to other LinkedIn invitations you've received.

Yes, the phish in Figure 1-19 is a good one. If it really is a clone, there won't be any indicators in the language, format, or branding that will give it away. In this case you'd have to do a little more investigating.

- Check the links to see where they go (once again, *check* does not mean *click*!).
- Confirm whether the address this e-mail was sent to is the one connected to your LinkedIn account (critical-thinking check).
- If you're extra paranoid, ignore this e-mail and log in to your LinkedIn account to see if there's an invitation waiting for you.

The example in Figure 1-20 is one that a friend of mine received. Getting an e-mail from AT&T was not unusual because the company is his cell phone carrier. Fortunately for him, he's a paranoid security type and thought to check on some things before he reacted. I would definitely call this one an advanced-level phish.

Now, I don't know if the e-mail in Figure 1-20 is an exact clone of an AT&T e-mail, but I can tell you that if it's not, it's *really* good. Some things that probably would have made the average user click include the following:

- Use of AT&T logo, colors, and images
- No obvious problems with grammar, spelling, punctuation
- The pretext of voicemail being inaccessible, which is something that most of us would take immediate action on

So what are some things that kept my friend from becoming a victim?

- It took him a minute, but he realized that the e-mail address at which he received the message was not the one associated with his AT&T account. This was the one thing that really saved him.
- There's no personal greeting in the message.
- The e-mail includes exactly *one* bad link! My friend checked all the links and found something very interesting. *All* of the links except the one link to retrieve the message were legitimate. So if he had not been thorough, this would have looked like a real e-mail.

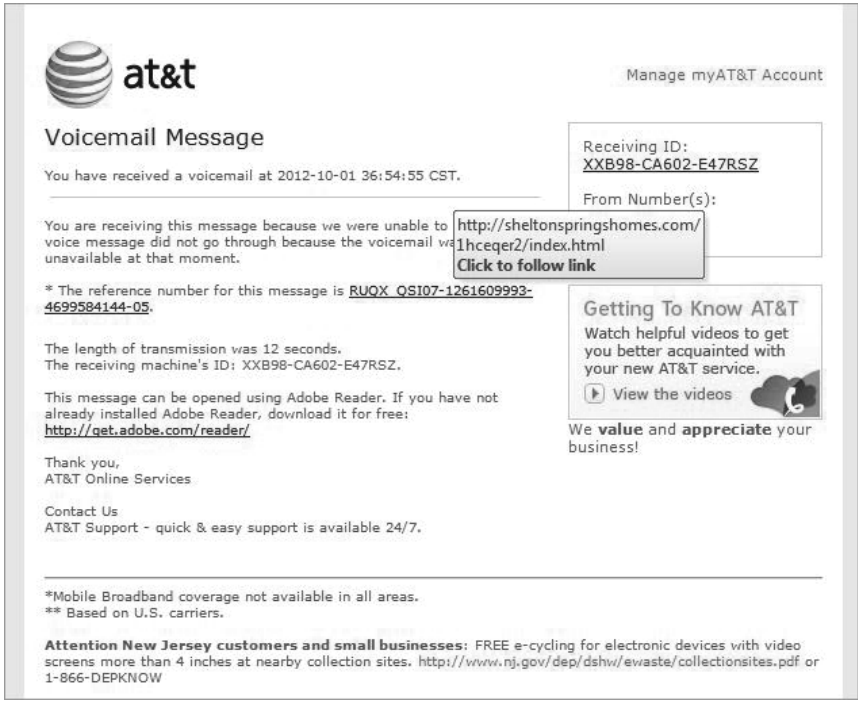


Figure 1-20: Advanced AT&T phish

Clearly the AT&T example is very difficult to identify as a scam; it definitely passes the basic sniff tests. Fortunately, my friend is in the habit of never accessing any accounts through e-mailed links. Hopefully after finishing this book, you'll at least rethink your habits.

Spear Phishing

To finish out this chapter, let's talk about the spear phish. Again, this is a phish that has been personalized to a specific recipient. The attacker has taken the time to get to know you; at a minimum, he knows your first name, last name, and e-mail address. Depending on how important you are, he might know a lot more than that. By doing just a few simple searches, he could find you through social media, your company's website, or anything else that you've participated in online. If you're really important, he'll know all about your hobbies, your interests, and what properties you own; he might even have knowledge about your family. Heck, if he finds anything really bad or embarrassing, he might not even have to disguise his attempt to get what you have. At that point, he

could just use that information to extort money or get you to data mine information for him. But I digress. We're talking about phish.

As creepy as it is, it's this level of research that can create a phish that's very difficult to resist. An attacker that really wants what you have won't hesitate to play dirty. He'll find out if you recovered from a severe illness and are now an advocate for that charity. He'll know if you like to gamble online or if you have a mortgage that's too big for your paycheck. This is really the heart of a spear phish. It's personal.

Figure 1-21 is an example of a spear phish that was making its rounds to top-level executives fairly recently.[15] Can you imagine getting this in your inbox?


From: United States District Court [subpoena@uscourts.com]
To: [redacted]
Cc:
Subject: Subpoena in case #28-755-YCH

AO 88(Rev. 11/94) Subpoena in a Civil Case

UNITED STATES DISTRICT COURT

Issued by the
UNITED STATES DISTRICT COURT

Issued to: [redacted]

SUBPOENA IN A CIVIL CASE

Case number: 28-755-YCH
United States District Court

YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below.

Place: United States Courthouse
880 Front Street
San Diego, California 92101

Date and Time: May 7,2008
9:00 a.m. PST

Room: Grand Jury Room

Figure 1-21: Spear phish

Let's do one final breakdown for the e-mail in Figure 1-21. What makes this a compelling message?

- It uses the U.S. District Court logo.
- It plays on fear and respect for authority. Who is ever happily surprised to be subpoenaed and COMMANDED to appear?
- It's personalized to a full name, e-mail address, business, and telephone number.
- It includes a time constraint. There's a date and time the recipient must appear—or else.

- It doesn't have any obvious typos or grammar errors.
- The sender is plausible: `subpoena@uscourts.com`.

In all honesty, I think this e-mail would be a very difficult catch for just about anyone. The following are only two indicators that I could find:

- The link to the subpoena is malicious. In this example it led to a site that downloaded key logging malware.
- The From e-mail address is `@uscourts.com`, which looks plausible except that the courts fall under a `.gov` top-level domain (TLD).

That's it! Two chances to get it right with a message that's going to create at least some anxiety and the pressure to act. So, once again, unless you have good habits ingrained, this one might have caught you.

Summary

Well, you've now been introduced to the world of phishing. At this point, you should know the following:

- The definition of phishing
- Common targets/attackers
- Reasons people phish
- Techniques used by scammers
- Examples of high-profile breaches started by phishing
- Common everyday examples of phishing
- Overview of difficulty levels

I hope you have a better understanding of what phishing is, the scope of it, and why it's becoming a bigger and bigger problem for all of us.

Let me just conclude this chapter with a few hard numbers. In just a small snapshot in time from May 2012 through April 2013, more than 37 million users reported phishing attacks. That's *reported to one source*, so these are only the ones we happen to know about. It's estimated that close to 300 billion e-mails are sent every day, and of that number, 90 percent are spam and viruses.[16] Those numbers are absolutely staggering, and they really point to only one thing. If you have an e-mail address, you're going to get a phish at some time. It's as simple as that.

Get comfy, because from here on out, we dive into what turns out to be very dark waters. Phishing isn't just about what you click, it's about

why you click it. We're going to get under the hood of the human OS and see what makes it tick. Sounds like fun, right? Race ya there.

Notes

1. Geoffrey Ingersoll, "Inside the Clever Hack That Fooled the AP and Caused the DOW to Drop 150 Points," November 22, 2013, http://www.businessinsider.com/inside-the-ingenious-hack-that-fooled-the-ap-and-caused-the-dow-to-drop-150-points-2013-11.
2. Tim Wilson, "Report: Phishing Attacks Enabled SEA to Crack CNSS's Social Media," January 1, 2014, http://www.darkreading.com/attacks-breaches/report-phishing-attacks-enabled-sea-to-crack-cnns-social-media/d/d-id/1141215?.
3. Andy Greenberg, "How the Syrian Electronic Army Hacked Us: A Detailed Timeline," February 20, 2014, http://www.forbes.com/sites/andygreenberg/2014/02/20/how-the-syrian-electronic-army-hacked-us-a-detailed-timeline/.
4. Danny Yadron, "Alleged Chinese Hacking: Alcoa Breach Relied on Simple Phishing Scam," May 19, 2014, http://online.wsj.com/news/articles/SB10001424052702303468704579572423369998070.
5. Brett Logiurato, "The US Government Indicts 5 Chinese Military Hackers on Cyberspying Charges," May 19, 2014, http://www.businessinsider.com/us-china-spying-charges-2014-5.
6. Symantec Official Blog, "Francophoned—A Sophisticated Social Engineering Attack," August 28, 2013, http://www.symantec.com/connect/blogs/francophoned-sophisticated-social-engineering-attack.
7. Anti-Phishing Working Group, "Phishing Activity Trends Report, 2nd Quarter 2014," August 29, 2014, http://docs.apwg.org/reports/apwg_trends_report_q2_2014.pdf.
8. Michael Riley, "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," March 13, 2014, http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data#p1.

9. Brian Krebs, "Email Attack on Vendor Set Up Breach at Target," February 12, 2014, http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/.
10. Aviva Litan, "RSA SecurID Attack Details Unveiled—Lessons Learned," April 1, 2011, http://blogs.gartner.com/avivah-litan/2011/04/01/rsa-securid-attack-details-unveiled-they-should-have-known-better/.
11. Nicole Perlroth, "Study May Offer Insight into Coca-Cola Breach," November 30, 2012, http://bits.blogs.nytimes.com/2012/11/30/study-may-offer-insight-into-coca-cola-breach/.
12. Sarah Perez, "AP Twitter Hack Preceded by a Phishing Attempt, News Org Says," April 23, 2013, http://techcrunch.com/2013/04/23/ap-twitter-hack-preceded-by-a-phishing-attempt-news-org-says/.
13. Casey Hill, "Email 'from Target' to Customers Is a Phishing Scam," December 20, 2013, http://www.marketwatch.com/story/scammers-pounce-on-target-fiasco-2013-12-20.
14. Jovi Umawing, "Fake CNN Spam Use Boston Marathon Bombing as Lure," April 18, 2013, http://www.threattracksecurity.com/it-blog/fake-cnn-spam-use-boston-marathon-bombing-as-lure/.
15. John Markoff, "Larger Prey Are Targets of Phishing," April 16, 2008, http://www.nytimes.com/2008/04/16/technology/16whale.html?_r=0.
16. Social-Engineer Infographic, April 28, 2014, http://www.social-engineer.org/resources/social-engineering-infographic/.