

# Phishing for Phun and Profit

*Phishing* is automated identity theft. It combines the power of the Internet with universal human nature to defraud millions of people out of billions of dollars. This is no exaggeration. Gartner, a research group in the IT industry ([www4.gartner.com/Init](http://www4.gartner.com/Init)), estimated in April 2004 that 1.78 million Americans had already given their information to phishers. And April was, quite frankly, the early days of phishing in the United States. Gartner's most recent estimate of the cost to U.S. consumers and industry is \$2.4 billion.

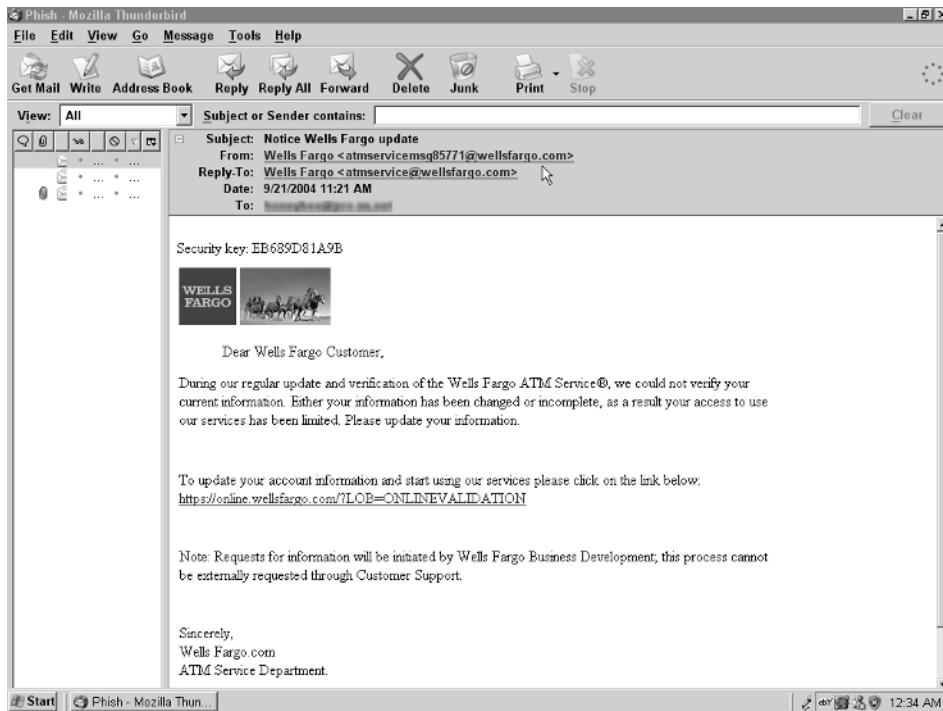
Nearly everyone with an email address has received a phishing email by now. These emails use the formatting and appearance of a legitimate business's Internet presence to trick you into providing your personal information. That information might be the username and password for your Internet banking account, your credit card number with expiration date and security code, your Social Security number (SSN), or other data. We all know better than to give these out without reason, but the phishing emails make it seem that we have good reason. After all, where's the harm in providing information that the organization already has?

The harm is that you're not talking to the real organization. The information you provide can be used to access your accounts, make transactions without your authorization, and even create new accounts. This is *identity theft*, widely reported as the fastest-growing crime today. Identity theft is widespread and

dangerous. People have found thousands of dollars of fraudulent charges on their credit cards; thieves have taken second mortgages out on their homes or mortgages on homes they never owned. People have tried to buy a car or house only to find their credit is worthless because someone else has ruined it. All this because someone has a little information on them—sometimes very little, as thieves have successfully taken out loans with completely random Social Security numbers, without even a correct name. Of course, having correct information makes it much more likely that an identity theft scheme will work.

Phishers know that the easiest way to learn something is to just ask, as illustrated in Figure 1-1.

The phishing email may contain a form to gather your information. It might use a hyperlink to take you to a website (see Figure 1-2) that looks like the website for the business that supposedly contacted you. The email may even direct you to call an automated phone script that sounds just like those menus you get stuck in when you call the business's customer service line. Some phishing emails infect your computer with spyware that sends your information to phishers when you type it into *legitimate* websites. If you do provide your information, you have set yourself up for identity theft, credit card fraud, or unauthorized transactions on your bank account.



**Figure 1-1** An example of a phishing email.



**Figure 1-2** A phishing website.

The businesses being impersonated include banks, Internet service providers, auction sites (okay, that pretty much means eBay, but other ones are being hit, too), Internet retailers (Amazon, ditto), and political campaigns. Their story line may be that your account has been fraudulently accessed, your account data has been lost, or you just won a new car! One particularly clever scam offered me a \$5.00 credit on my credit card if I signed up. Considering that my own credit card company has offered me cash for signing up for this or that, why would this email request make me suspicious?

Currently, only the largest and most prominent businesses are being impersonated. As time goes on, I expect the phishers to expand into smaller enterprises. The phishers don't know whether the people on the receiving end of their emails actually have relationships with the businesses they are misrepresenting; it doesn't matter. It takes so little work to send phishing emails to millions of addresses, and so little work to harvest the information, that even a few responses means a large profit. Estimates for phishing response range from 1 to 5%.

In addition, the use of Trojans and spyware is increasing. In these cases, victims don't even need to supply the information. Their computer is compromised and sends the information to the phishers on its own. A user who is smart enough not to enter her information into a phishing scam may still become infected with a keystroke logger that watches for usernames, passwords, and other personal

data. There's a new security exploit published every day, and assuming that you're immune because you're a geek or use a \*NIX-based operating system isn't wise. (Amiga users are mostly safe, though.)

The original use of all this phished information, back in the 1990s, was to steal AOL hours. A secondary use, known as *carding*, involved making unauthorized purchases with stolen credit card information. That's small potatoes. Now, the criminal infrastructure is developing to really use these stolen identities to drain bank accounts, max out credit cards, create *new* credit accounts, and then max them out.

Now we have all these too-good-to-be-true job opportunities: you know, the ones where you can make \$5,000 a week in your spare time! (I could do with that.) People are recruited through spam email or job boards to work for casinos or plasma TV resellers or charities. In reality, the phishers are enlisting intermediaries to launder the money stolen from phished accounts (see Figure 1-3).

These intermediaries are called *mules* because of the parallels with drug couriers. Once money is transferred from the victim's account to the mule's account, the mule wires it on again to the phishers, less a 5–7% commission. When legal authorities trace the funds, the trail stops at the intermediary, who may be arrested for receiving stolen funds depending on the laws in that jurisdiction. Again, millions of people see these ads; only a few dupes are needed to turn a profit.



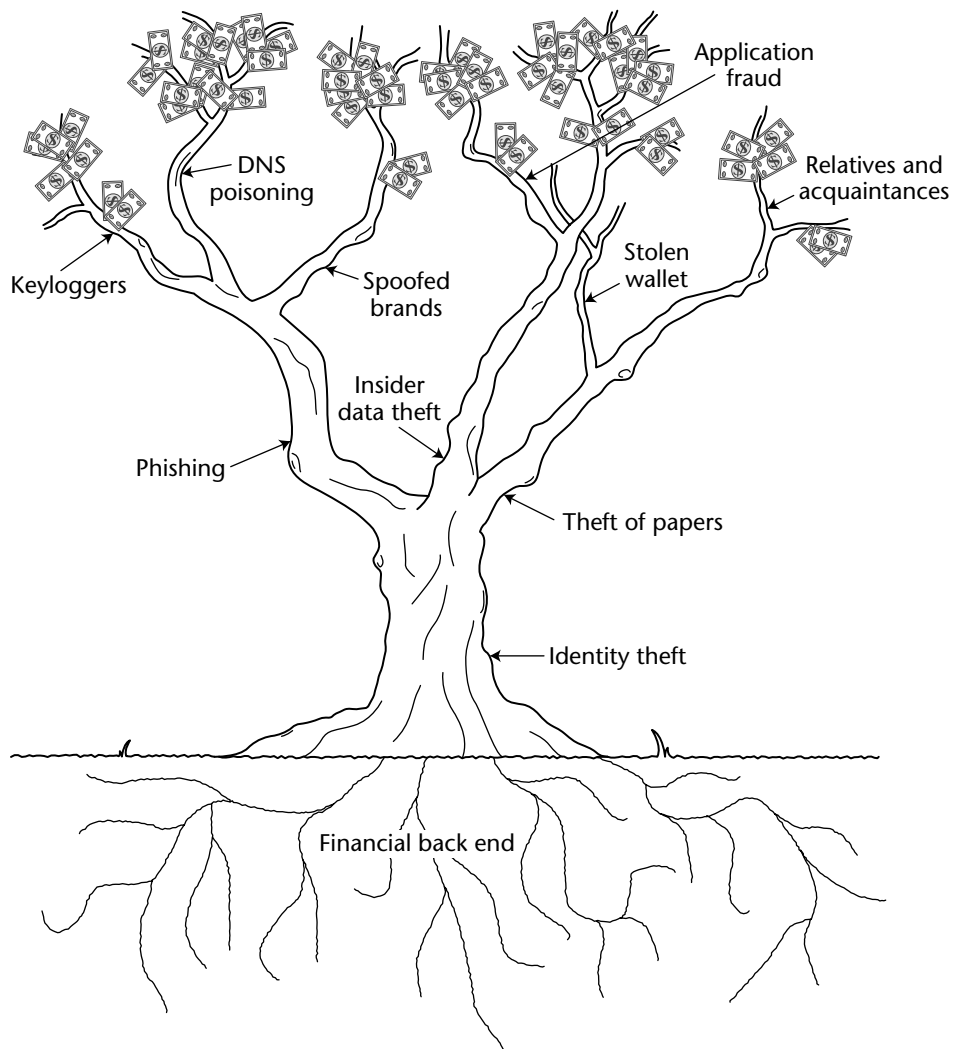
**Figure 1-3** A website for recruiting mules to launder money stolen through phishing.

## Why Go Phishing?

There is one very simple reason for phishing: money.

Identity theft is easy and nearly risk-free. Gartner reports that only 1 in 700 identity thieves are prosecuted. Phishing enables remote identity theft—no more dumpster diving or mail stealing needed to obtain the information. It's as if the money grew on trees!

Take a look at Figure 1-4. It's a silly picture that illustrates a very important point: Phishing is just one of the many ways to access the money available through identity theft. It's also one of the easiest and safest.



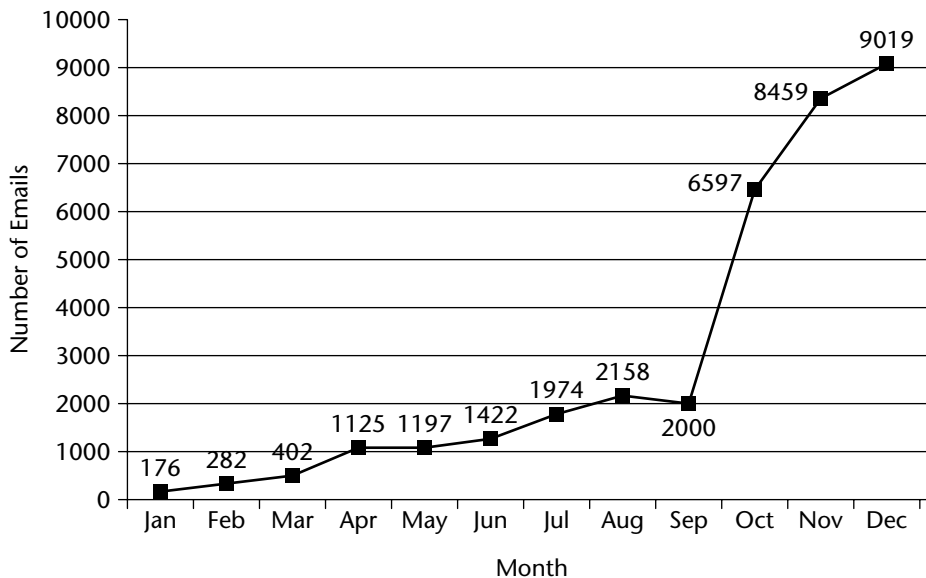
**Figure 1-4** The money tree.

Just how much money is available? I will leave that as an exercise for the student.

Why is all this happening now? Phishing isn't new, of course. The term was first coined sometime around 1995, when crackers would ask new AOL users for their usernames and *maybe* their passwords. In those days, you could usually crack the password if you had a name; it would be something like *password* or *abc123* or *sex*. (This is yet another reminder that bad passwords trump security.) However, phishing wasn't a major problem until the end of 2003. The Anti-Phishing Working Group ([www.antiphishing.org](http://www.antiphishing.org)), an industry association, reports only 176 phishing incidents for January 2004. By contrast, there were 1197 reported in May. That's nearly a 600% increase. Gartner's study in April 2004 found that three-quarters of the attacks people reported have happened since October 2003. Figure 1-5 shows just how fast phishing grew in 2004.

The Internet has reached critical mass. Enough people have moved enough of their lives online to make this avenue of attack worthwhile. The costs are enormous for businesses and victims; unfortunately, the consequences for phishers, if they're even caught and prosecuted, are minimal. Many work in countries with few, if any, laws regulating the digital world. The scam will continue.

**Unique Phishing Lures Reported in 2004**



**Figure 1-5** Phishing lures increased an average of 56% per month in 2004.

Copyright Anti-Phishing Working Group ([www.antiphishing.org](http://www.antiphishing.org)).

The businesses affected—and the governments they pay taxes to—are noticing the problem and working to stop phishing in its tracks. I'm not optimistic, frankly; the phishers are using the easy techniques they're using now because they *work*. If we manage to make it so they don't work, the phishers will just go on to schemes that are more difficult to execute and to prevent. Why shouldn't they get the easy money while they can? It will take real changes to the system to protect consumers, and those changes are expensive and difficult.

## It's Everyone's Fault

---

Ten years ago, when Internet commerce was just getting started, we (techies, I mean) spent a lot of time convincing timorous relatives that yes, it really is safe to order our birthday presents from Amazon. We were comfortable with the Internet and wanted, for a variety of reasons, to share that comfort with our friends and family. The Internet is *neat*. I'd really rather send my grandparents email—they get to hear from me more often that way. The convenience and cost savings of email, online ordering, online banking, and other cool stuff is irresistible. Now I'm wondering if maybe we should have resisted. Then I realize how much identity theft happens *without* phishing and I get over it: e-commerce is only a little more dangerous than regular commerce.

Of course marketing—the drive for faster, prettier, shinier websites and applications—shares a lot of the blame. In order to convince people it was safe, we made it ever easier to ignore or circumvent security precautions. How many times have you clicked past an expired or badly formed certificate? Large corporations want the cost savings and the responsiveness of Internet business. The marketing paradigm has become *If you link it, they will come*, and links have been added to everything from emails to magazines to white papers, even while security experts hop up and down saying “Don't click!” Many corporate websites include ActiveX, Javascript, Flash, and other add-ins to plain HTML—all of which have been used to carry malicious code.

There's a lot to be said for the anti-Microsoft stance, too. I don't want to start a religious argument, but the facts are pretty damning. Many of the security flaws now being exploited are found in Microsoft code. Microsoft has worked very hard to become the dominant desktop operating system, and it needs to take more responsibility for its ubiquity. Just because security flaws are found in \*NIX systems (including Macintosh) doesn't change the fact that Windows is what most people use and depend on. The automated nature of phishing attacks means that they target the most common systems available: Windows, Outlook, and Internet Explorer. In June 2004, CERT began recommending switching to a different browser because of a dangerous vulnerability in Internet Explorer (IE). If and when another system becomes as widely used as IE, I hope we'll hold that system's vendor to the standard I'd like to hold Microsoft to now.

Finally, the back ends of our banking and credit systems are a mess. These systems are predicated on the fact that only you know your name, date of birth, Social Security number, and account numbers; therefore, someone who knows all this is authorized to make changes to your accounts, open new accounts, and so on. On the other hand, there is a multibillion-dollar industry dedicated to compiling as much information about you as possible in order to market to you more effectively. Huge databases offer lawyers, collection agencies—anyone who is willing to pay—your name, Social Security number, previous addresses, relatives, associates, and so on.

We are routinely asked for all sorts of information, so it's difficult to grasp how dangerous this information can be in malicious hands. My theory is that this is so difficult to understand because it's mind-bogglingly silly. Someone really can make up a Social Security number and steal the credit history of the person who happens to have that number, whether or not the person has the right name, is living at the address the thief gives, or is even alive. Your credit report is regularly polled in order to send you preapproved credit offers and special deals; employers ask for your SSN on job applications; utility companies pull a credit report before allowing you on the grid.

And now that I've offended techies, marketers, capitalists, and Microsoft, I feel like I've properly begun.

---

## Terms

---

*Phishing* is a made-up word, and the way it fits into the English language as a particular part of speech hasn't quite settled in yet. For the sake of consistency, here is how I use *phishing* and related terms throughout this book:

**Cracker:** A criminal hacker or black hat; someone with the skills and knowledge to develop serious computer attacks. *Crackers and hackers are different.*

**Hacker:** Someone who is smart about computers and likes breaking systems but doesn't necessarily do so for criminal purposes. *Hackers don't like it when they're lumped in with all computer criminals.*

**Mule:** Someone whose account is used to launder phishing money; the term comes from slang for drug couriers. *The mules get arrested, but the phishers go free.*

**Phish:** A victim who provides information to a phisher. *My poor sister's a phish!*

**Phisher:** A criminal who sets up a phishing scam. Used in the singular for convenience; many phishing scams seem to be the work of criminal organizations. *Are phishers more like script kiddies or mafia?*

**Phishing:** The act of obtaining personal information directly from the end user through the Internet. *They say phishing is a serious crime, but it's pretty easy to get away with it.*

**Phishing email:** An email sent to potential phish. *Nearly half my spam is phishing emails now.*

**Phishing scam:** A set of activities—usually an email and a website, but sometimes many emails and websites, macros, phone scripts, and so on—designed for phishing; a single attack, from planning through execution. *A phishing scam may involve several different email campaigns and web servers.*

**Phishing spyware:** Spyware used to pick out personal information (as opposed to, say, the kind that tracks your web visits) in a phishing scam. They can range from keyloggers to sophisticated little programs that watch for what websites you're visiting. *I think phishing spyware is L33T (elite).*

**Phishing website:** A website that collects a phish's personal information. *Phishing websites are so cute!*

**Script kiddie:** Someone who uses scripts and programs developed by others to attack computer accounts and find vulnerabilities. The script kiddies generally don't understand the scripts they are using or the extent of the damage they can inflict. *Script kiddies can really cash in on phishing.*

**Spoof:** To pretend to be something you are not, whether by looking like that something (as in spoofed websites) or by pretending to have the same origin (as in spoofed *From* addresses on emails). Some people call phishing *spoofing*; I don't. I think the spoofing part is a red herring, and the real issue is the information gathering. Many kinds of Internet forgery are called spoofing. *Phishing scams often used spoofed emails and websites to trick you.*

## **Phishing Scams**

---

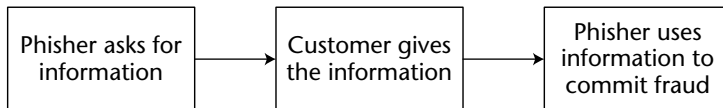
As I write this, the most common scam is a claim that your account has been used fraudulently and will be closed unless you verify your personal information. This is not the only kind, however. Some say that the information has been lost; others ask for a "routine" verification of your information; still others claim you've won a free car. *Anything* that gets you to click a link can take you to a spoofed site.

One major bank, hard hit by phishing, began maintaining an archive on the web of all their legitimate emails. Guess what happened? Yup. The phishers started using the same email messages so that even *more* customers were fooled. If the victim conscientiously questioned an email, the web archive assured the phish it was okay. So the bank took the archive down.

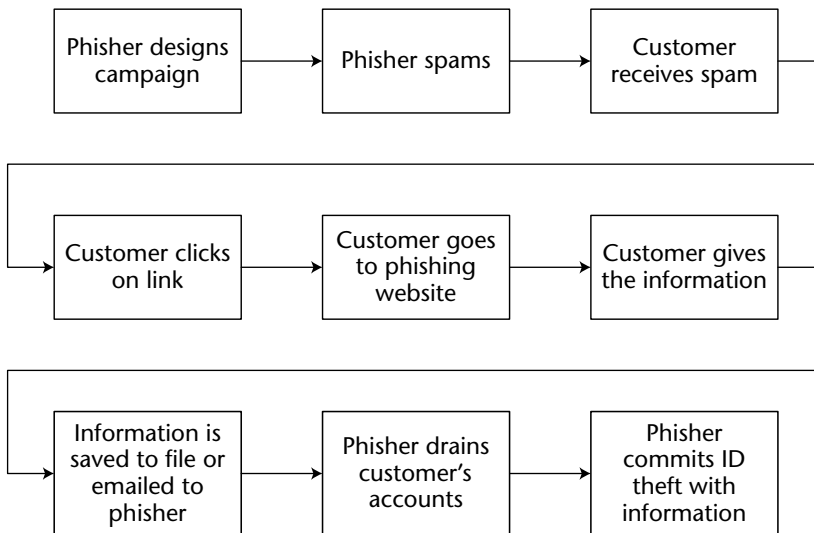
A phishing scam, however, starts well before the email is sent out.

## What Happens in a Phishing Attack

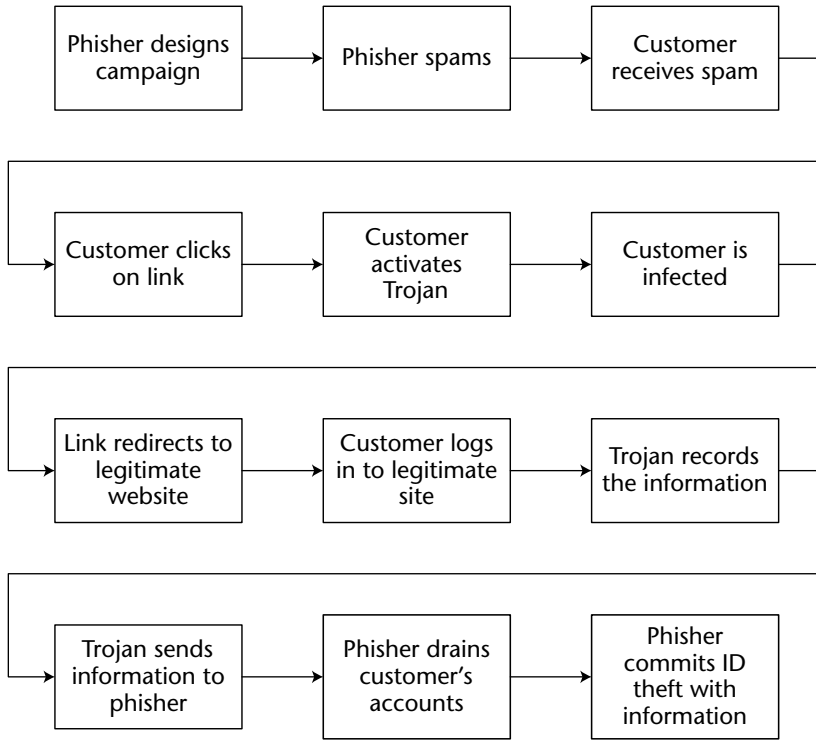
There's a basic plot to the phishing story, just as movies and books have a basic plot. In narrative, it's called a *throughline*. Phishing scams can be very complicated, so here's a simplified version:



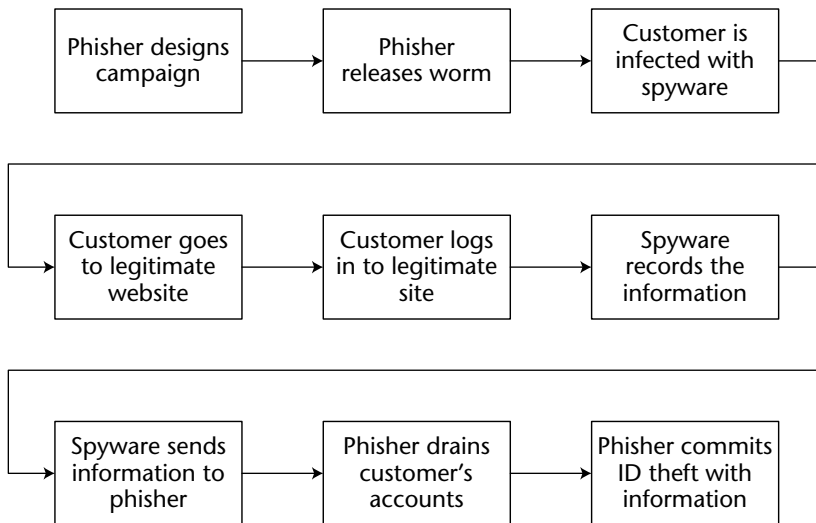
Maybe that's too simple; here's how the usual email + website scam works:



And here's a prototypical spyware-based scam:



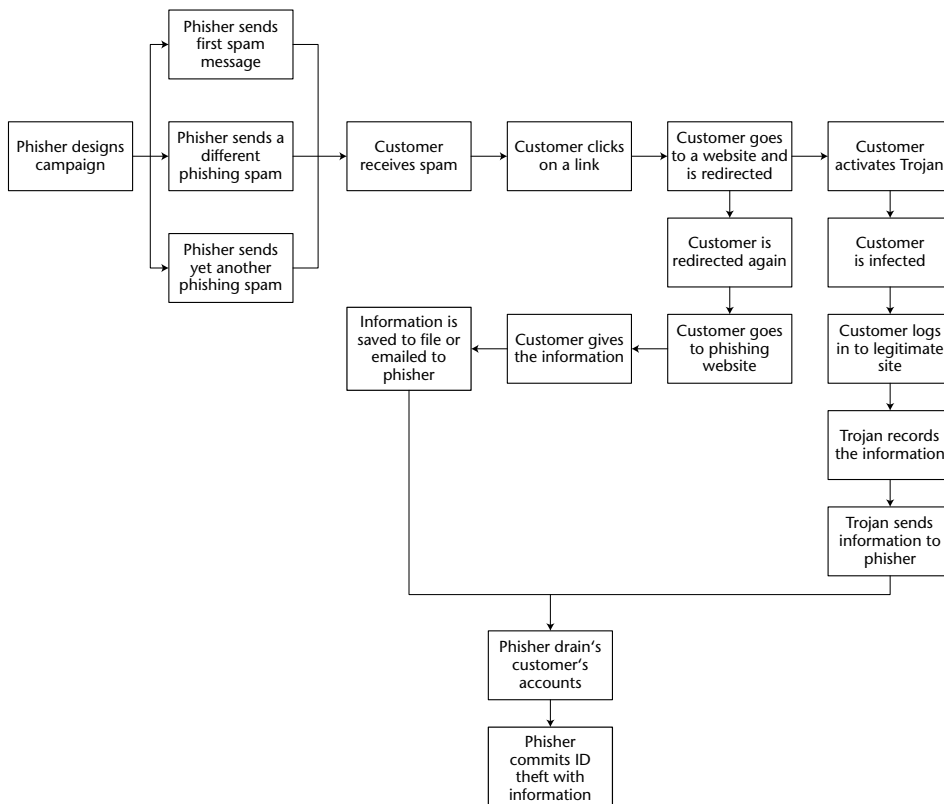
There are a number of variations on the spyware scheme. Here's one example:



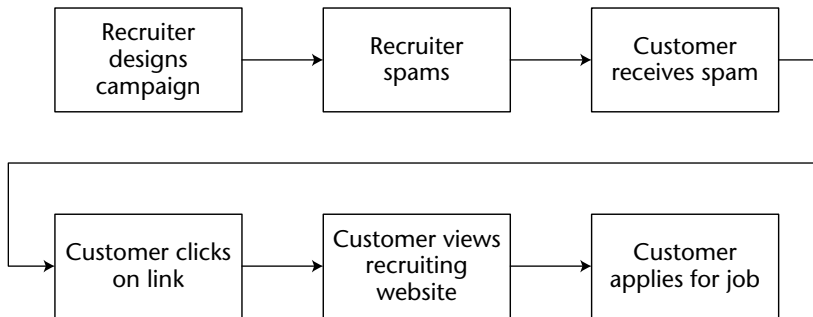
This last one is the one that makes me want to tell folks to put their money in the Bank of Sealy Posturepedic Mattresses. Will it happen? It already has.

On May 28, 2004, F-Secure reported that the Korgo network worm—a worm that spreads without user intervention using the Sasser vulnerability in Windows—was spreading and sending bank usernames and passwords to the mothership. It also sent back everything infected users typed into a form, which would include credit card numbers, passwords, and so on. Korgo is a nice, slow little worm, and many systems were already patched because of the effects of Sasser. Still, it's working away across the Net and is now up to variant U (having already gone through A, B, C, and so on). Chapter 4, talks about cross-platform spyware and what a really aggressive worst-case worm can do.

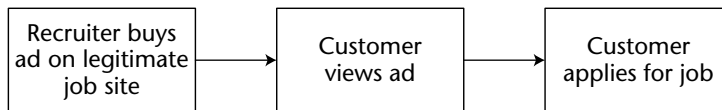
Real phishing schemes are often more complicated than the ones just shown, however. For example, multiple phishing emails—sometimes for different spoofed institutions—can point to the same website. The phisher can use redirects to send someone between various websites before landing at the final server. That way, if any one server is taken down, the phishers can route around it. Here's a complicated scam, a little more realistic than the simple schemes I just showed you. Although we don't know for sure whether email and spyware scams are perpetrated by the same or different groups, it wouldn't surprise me if they both came from the same source.



The throughline for recruiting mules works like this:



Or maybe this:



## Who Is Doing the Phishing?

It's generally a good idea to know your enemy. Just who are the people phishing for your personal data?

It's a pretty broad cross-section of the digital underground, from script kiddies playing with phishing kits and carding to foreign mafia who have found a whole new, wide-open realm for exploitation. There are phishing communities and chat sites that discuss what works, what doesn't, and who the easy and hard targets are. A friend monitors them as he finds them, and the amount of information shared is unnerving. The image of the Lone Hacker bravely confronting corporate interests, seeking intellectual challenge and mischievous, mostly harmless fun, doesn't apply here.

Given what's said on the phishing community sites, it seems that many phishers rationalize their behavior by saying they're stealing from the big corporations, not individuals. Someone who's been a victim of identity theft, however, might beg to differ.

### *Script Kiddies*

Script kiddies—the same children who use virus toolkits to spread malware and crack game codes so they can win at Diablo—are definitely in on the phishing wave. From the descriptions of early AOL phishing, I'd even say they

started it, which is the reverse of the usual situation. (Usually, a class of attack is started by people who know what they're doing; phishing for AOL users was so easy that *anyone* could do it.)

The standard phishing scam is pretty easy to execute, even for a script kiddie. Websites like CarderPlanet.com and ShadowCrew.com (those domains are down now, but I'm sure new ones have taken their place) sold phishing kits. Phish-in-a-box are available free on the Internet, enabling kiddies to put up a site in the time it takes to unzip the pages. Send out a spam email; compromise some random box out on the Internet with a root kit; put up a site. Then buy a neat new gaming computer or stereo with the stolen account information.

The script kiddie might even sell the identity to someone who can make real use of it. The going rate for reliable financial information of someone with \$50,000, according to a speech given by Dan Greer at the Workshop on Economics in Information Security in 2004, is \$500. Phished identities aren't worth as much because the provenance isn't as good. The point is that criminals are actively buying identity information. Whether or not you're initially taken in by an easy scam, you can still be in for a world of hurt.

### ***Serious Crackers***

Serious crackers (or gray-hat hackers who aren't picky about who they work for) can execute more sophisticated attacks than script kiddies. They can develop their own spyware, run tricky scripts through email or websites, compromise boxes that aren't left wide open, and generally wreak havoc. These are the people who develop worms and Trojans. They can perform far more elegant and dangerous compromises on potential server machines.

A cracker might have a *bot net* available: a collection of compromised Windows computers all writing home to mommy, asking for directions. These zombie machines will send spam, perform denial of service attacks, or seed worm infections. The best estimates put *millions* of computers as part of some bot network—anyone with an always-on broadband connection is a target. There are cracker and virus wars as various bot controllers try to take over each other's zombies. It would cost \$1 per *month* to rent a single bot for my own nefarious purposes. If you consider the value of something to be its market price, that's how easy it is to buy someone else's computer to do your bidding. Your computer is worth \$1.

And what do you want to bet a lot of those zombie computers are running phishing spyware?

### ***Organized Crime***

Criminal syndicates are responsible for the most elaborate and thorough phishing scams. These are the people who hire the serious crackers. They

develop fancy websites to recruit mules for money laundering. They can create fake credit and ATM cards with your information and use them in any store or ATM. These are the people who do the most damage to victims.

The worst thing that can happen is for your information to get into the hands of an organized crime network. They have the skills, tools, and manpower to thoroughly trash your identity. They can drain your bank account, open up new credit cards, max those out, get driver's licenses and passports in your name, use your job history to gain employment. . . . Get the picture?

### **Terrorists**

Currently, there are no direct reports that terrorist groups are profiting from phishing. They are, however, profiting from identity theft. In 2002, the FBI stated the following in congressional testimony:

*The impact [of identity theft] is greater than just the loss of money or property. . . . Terrorists and terrorist groups require funding to perpetrate their terrorist agendas. The methods used to finance terrorism range from the highly sophisticated to the most basic. There is virtually no financing method that has not at some level been exploited by these groups. Identity theft is a key catalyst for fueling many of these methods.*

For example, an Al-Qaeda terrorist cell in Spain used stolen credit cards in fictitious sales scams and for numerous other purchases for the cell. They kept the purchases below the amount where identification would be required.

So many people cried *cyberterrorism* after the attack on the World Trade Center in 2001 that the term has gone out of fashion. Nevertheless, it's a problem that needs consideration. If nothing else, the idea may free up some money for law enforcement.

If terrorists aren't using phishing for funding yet, they will be—it's just a matter of time. Terrorist groups have worked with organized crime in the past to fund their operations. Interpol reported that the Chechen mafia worked with Chechen terrorists in a counterfeiting scam, and it was widely reported in the Associated Press and elsewhere that France's top antiterrorism judge had determined many terrorist cells were using stolen credit card information to finance their operations.

Terrorists work with organized crime to raise money; terrorists use identity theft to raise money; organized crime uses (among other techniques) phishing to commit identity theft. Is this what they call *connecting the dots*?

### **Where They Come From**

Many phishers are not citizens of first-world countries. If they are, they tend to be of the script-kiddie variety, not the organized crime variety. The laws against

white-collar crime in first-world countries are generally more stringent, which provides some deterrence, and first-world countries tend to have better police and more ways to find you. And besides, if you're local, there are other ways to steal money—you have physical access.

Don't assume that because phishers are often from second- or third-world countries they're stupid; likewise, don't assume that lousy English means the writer is foreign. Many customer education pieces I've read say that phishing emails are written by "foreigners," and that's why there are so many errors. First of all, the number of errors has gone way down as people have wised up. Second, if a badly worded email still hooks phish, why go to the effort of fixing it? Maybe people who don't notice poor grammar won't read their bank statements, either. Some phishers *pretend* to write broken English to mislead readers into thinking they are uneducated. I have seen speakers in phishing communities use poor English in one sentence and perfectly good English in the next.

That said, the major sources for phishing scams appear to be Brazil and Eastern Europe. UK security company m2g reports that Brazil is the capital and main exporter of hacking activity worldwide, while Eastern Europe is the center for malicious code and criminal syndicates creating identity theft scams.

The former Soviet nations tend to have excellent educational systems and high poverty rates—a dangerous combination. The local governments have been trying to crack down, but there is enough corruption in the ranks that they're not getting very far. Authorities in Romania have arrested 100 phishing hackers, and that's just a drop in the bucket. I've noticed that the gentleman all the news stories cite, Dan Marius Stephan, is serving all of two and a half years in jail for stealing US\$500,000.

Brazil is an especially dangerous threat. Several studies say that the entire nation is a laboratory for crackers. *H4CK3R* magazine is a white-hat publication, and it's widely available on newsstands throughout the country—there's a lot of interest in playing with code. In a nation where the average wage is US\$300 per year, most people don't have access to computers; those who do are a fairly close-knit community. They share information and techniques far more than the stereotypical "lone hacker" we're used to. In addition, Brazilian law holds that hacking and intruding into systems is not in itself a crime—you have to be proven to have done something criminal with your computer skills to be prosecuted. This means that there is almost no deterrence.

The Middle East is currently behind Brazil and Eastern Europe, but it's starting to catch up. Given the terrorist movement and its need for financing, combating and preventing Middle-Eastern cracking should become a major priority.

When Russia made it into space before we did, the U.S. instituted a nationwide program of science education and raced to beat them to the moon. I suppose it's too much to hope that we'll fund a major educational initiative to catch up in hacking skills.

## Who Is Targeted?

There are several targets in a phishing scam: the end user, the businesses being spoofed, the computers compromised to host fraudulent sites, and the ISP hosting the email address. The end users—the phish—get their identity information stolen. Everyone else is used in an attempt to get to the phish.

### ***End Users***

The end user is potentially every person with a bank account or credit card and a computer on the Internet in any nation that has a credit system.

Citizens of developed countries are more of a target than those in third-world nations because their banking systems are more robust, they have more money, and besides, they don't deserve their good fortune in being born in a rich nation. While I concede that I didn't deserve my good luck, I don't understand why that means I do deserve to have my bank accounts drained and my credit destroyed. I'm sure that the phishers could explain it.

According to one ISP, the average phishing victim loses \$300. According to Gartner, identity theft victims lose \$1200, not to mention all the time they have to spend clearing their name. As you can see, the estimates of the costs vary widely. The \$300 estimate was reported rather early in the phishing phenomenon, and those who find out about identity theft sooner usually manage to lose less. Let's just take from this that people actually do lose money.

It's probably useful to note that phishing victims are a subset of identity theft victims. Phishing attacks currently only work against people who engage in commerce online, which pretty much requires them to have a credit card or bank account. Identity theft targets every individual, living or dead, with accounts or without, in a nation with a credit system.

Moreover, not all phishing scams will get as far as identity theft—so many identities are phished that the phishers currently don't manage to commit fraud against all of them. Doubtless they are working to increase capacity.

### ***Businesses***

Any business you can think of can be spoofed. The Anti-Phishing Working Group (APWG) divides such businesses into four sectors: financial services, retail, ISPs, and miscellaneous.

#### **Financial Services**

Financial services include banks, credit card companies, and PayPal. The main reason to phish a bank's customers is to get access to their checking and savings accounts—you don't have to just settle for the identity information and

credit cards. Fraudulent use of accounts is where the banks are hardest hit, and they are working to minimize their losses. Unfortunately, this may include refusing to cover consumers whose accounts are hijacked.

Everyone likes to phish Citibank; it usually wins the dubious distinction of being the most phished enterprise in the APWG's monthly reports. Although you should take this with a grain of salt because reporting isn't standardized yet, those numbers are as good as anything available. PayPal, U.S. Bank, Fleet, and Lloyd's are also hard hit.

Citibank is trying to make lemonade out of lemons, and has developed ad campaigns designed to educate consumers *and* assure them that they'll be taken care of. I have to admire the chutzpah required to claim that a high incidence of identity theft is a reason to keep my money at Citibank. They're right, however, that it's not really the bank's fault that phishers target their customers—it's just that they have so many customers.

### **Retail**

The retail sector includes eBay (second only to Citibank) and, well, eBay. Amazon also gets some phishing attacks. Traditional retail outlets are not favored by phishers because they get only the credit card information without also gaining access to the bank account.

However, eBay auctions are ideal for the phisher because of eBay's reputation system. Sellers and buyers who complete transactions honestly earn good feedback. By using someone else's eBay ID, the phisher can create fraudulent auctions using the phish's good feedback score.

There is an entire cottage industry of fraud that has sprung up around eBay. If a potential customer worries about sending large sums to the seller, he can be directed to one of many fraudulent escrow services that pretend to hold his finances safely until the transaction is completed. In reality, those escrow sites harvest the information and keep the buyer's money. Thousands of dollars worth of business can be done before the stolen identity acquires enough negative feedback to warn buyers.

### **Internet Service Providers**

Citibank may be the most phished enterprise, but AOL has been dealing with the problem, off and on, for 10 years and counting. This, if nothing else, is what convinces me that phishing is here to stay. If it couldn't be solved in the last 10 years, it's not going to be solved now.

Other ISPs being phished include Earthlink, MSN/Hotmail, and Yahoo!

## **Phishing Paraphernalia**

Most phishing scams need a place to host the files used to spoof the businesses—the website, the images, the scripts—and all of them need somewhere to store

the phisher's stolen data. The latter can either be a compromised box (explained in the following section)—the same as that hosting the phishing website, or a different one—or an email account. The email account doesn't necessarily need to be free, but it often is because those are anonymous.

### ***Compromised Boxes***

As the earlier discussion of bot nets should demonstrate, there's no shortage of insufficiently secured computers on the Internet that phishers can take over. A single phishing scam will often compromise several different computers: one or two for redirects, one or more for actual sites, and yet another to collect information. Round-robin DNS entries can help spread the load across servers; if one site is brought down, the next one may still be up. The compromised computer doesn't have to be a server. Any always-on computer connection means that the phisher can set up web services.

There aren't any good numbers on whether more Windows or \*NIX boxes are compromised for phishing websites. I would like to be able to say that of course Windows machines are much easier to own, but there are plenty of Linux computers out there that have been taken over. I've never heard of a Mac OS machine being used, but that doesn't mean that it isn't possible. It just means that they're not common enough for phishing kits to be in wide circulation.

Phishing websites can be hosted on all kinds of systems. I've seen them hosted by individual home users, small businesses, elementary schools, small-town chambers of commerce, web hosting companies, and just about anything else you can think of. It's hard to say what proportion of compromised servers belong to organizations that presumably have someone managing their networks, but it's clear that they do form a significant percentage of the lot.

Using information from APWG, it's clear that a plurality of compromised computers is in the U.S. We have a wealthy nation in which a lot of people can afford computers, combined with the fact that a great many users are true novices with little or no formal training in using them. They frequently don't know how or why they need to protect themselves. I expect that other nations also have a great percentage of novice users on the Net, but the U.S. wins by the sheer number of citizens with access. Lots of people—38% of American households as of 2004—have broadband through DSL or cable, and the ISPs don't seem to pay much attention to the safety of their consumers or the Internet they have inflicted them on.

South Korea and China are the countries with the next highest number of phishing websites. These countries have a lot of computers and expanding access to broadband. The language barrier between them and the Western nations targeted by phishing scams, and the time zones that mean your staff is asleep when their staff is awake, and vice versa, can make phishing sites difficult

to deal with. On average, phishing sites in the Far East stay up twice as long as phishing sites in North America.

There's an inverse correlation between the number of compromised phishing servers in an area and speed of shutdown. As the domain registrars and holders of large IP blocks get used to phishing, they get faster at shutting sites down. The average amount of time a phishing site stays up, as of June 2004, is 54 hours according to the APWG. If you have a good team of incident response people shutting sites down, you can get that much lower. Some sites, however, still stay up for weeks.

### ***Free Email Accounts***

Sometimes, instead of saving the phished data to a compromised server, the phisher has it emailed to an anonymous (and therefore free) account. There may be one or two email forwards going on, as well. Yahoo!, Hotmail, Juno, and other free ISPs have all been used for this. Although I haven't seen a Gmail account used as of this writing, I won't be surprised at all when it happens.

## **The Other Kind of Phishing**

The phishing discussed in this book isn't the only kind of phishing out there. This book is about obtaining identity information from the end user through the Internet. Phishers email anyone and everyone in hopes of getting a hit. However, the identities—and credit ratings—of random Internet users aren't the only thing phishers might be after.

Phishing is just a mechanism, so it can also be used to obtain other kinds of information, such as the usernames and passwords of a particular company's employees that the perpetrators might then use to break into the corporate network. This is a very different attack from identity theft phishing: it's targeted to a particular company, so it's a lot easier for a scammer to research the best way to appeal to the recipients and include specific, plausible information about the victims. The phishing emails could come from a forged internal address or the address of a business partner. The Cute Name Brigade has dubbed this "spear phishing." The purpose could be anything from compromising internal systems to industrial espionage.

Many people reuse their usernames and passwords, so it's also possible that phishers could use the bank account information they get to try to break into the victim's place of work. There is a real problem of scale here—correlating one victim's identity with his workplace is easy, but phishing has caught enough people that this wouldn't be worthwhile unless you could do it automatically. The means for doing this aren't quite available . . . yet.

Targeted phishing attacks are similar to the more general attacks that this book talks about. They might use many of the same techniques and have some

similar defenses. However, they differ in scale and purpose and they aren't necessarily performed by the same groups of people, so these very specific attacks are beyond the scope of this book.

## Account Fraud and Identity Theft

---

The main reason to phish is money. The next most important reason to phish is also money. The easiest way to get at money is to pretend you're the one authorized to get at it. Ergo, phishing for your account information. Ergo, identity theft.

The technical definition of identity theft—what many banks and credit card companies are insisting on—is “Using someone’s personal information to obtain new accounts in that person’s name.” There’s a problem with this definition from the layperson’s point of view. When I think of someone using my account information to drain my checking account, I call that *identity theft*. In my mind, the act doesn’t even have to lead to the opening of new accounts in my name. Technically, however, simply draining my account would be considered *account fraud*, not identity theft. This difference in definition matters because banks, in particular, want to treat account fraud differently from identity theft, probably with the hope of not having to pay the losses. After all, if you have been negligent, they may have grounds to refuse repayment.

Your credit card liability is legally capped at \$50. Your bank account liability, however, is capped at \$50 only if you report the losses within two days. If you report the losses after two days and before 60 days, they’re capped at \$500. After 60 days, you are out of luck. This is Regulation E, governing electronic transactions. Your bank may have better terms. Have you read them?

### Account Fraud

Account fraud is the first thing phishers do with your information.

If they phished your bank account, they’ll often wait a couple of days in hopes that you’ll have finished your panicked account checking. Some people, when they think they’ve been phished, quickly log in and check their accounts to see if anything has happened. But they may not think to change their passwords. Then the phisher uses online payments to send money to the mules’ accounts. The individual transactions are low enough not to trigger alerts, but the account gets drained. At some point—in a few days, at the next paycheck, or longer—you notice that the money is missing and ask for it back.

This can be a hassle. There are newspaper reports that some banks need to be threatened with lawyers in order to return the phished money. Banks refuse to reimburse you if they believe you were negligent. The federal insurance on

your account protects you only if the bank fails—it has nothing to do with fraudulent transactions.

You can find more details on how to deal with account fraud in Chapter 9.

## How Easy Is It to Steal My Identity?

How easy is it to steal an identity? Really easy. Everything is available to someone who knows how to look. Haven't you received those *Investigate Anyone* spams? Private eyes, lawyers, bill collectors, and criminals all know how to do this. There are no ways to prevent it—even dead people and children can have their identities used. If I have your name and address, I can get your Social Security number with a search on AccurInt or another personal database. From there, I can find almost anywhere you've ever lived. Did you apply to rent an apartment? Did you sign up for utilities? Then you had a credit check, and you can be traced. Where have you worked? Who are your relatives? The AccurInt website says this about its services:

*AccurInt allows you to instantly find people, their assets, their relatives, their associates, and more. You can search the entire country for a quarter—less than the cost of a phone call.*

Your AccurInt report has a lot more data than your credit report. And since LexisNexis admitted in March 2005 that the database was hacked, someone else may have that information, too.

When I say there's no way to prevent classic identity theft, I mean it. Phishing is just not that big a deal as far as classic identity theft goes. It just happens to offer a really, really easy way to get the information. There are lots of other ways:

- A crooked employee could sell your data.
- A major database could be compromised.
- A waiter could skim your card at a restaurant.
- Your roommate could copy your SSN from your college papers (this happened to my sister).

The FTC surveyed victims in 2003 and found that 9% had their identities stolen by relatives. Sure, people can sift through your trash, but the popular image of dumpster divers is not where the real threat is. Shred your documents for privacy, not protection. The real threats are your friends and family, and those large information databases.

The only thing that consumers can really do about identity theft is to carefully audit all accounts. Check your credit reports from all three bureaus twice a year; read your account statements every month. When you find identity theft, act aggressively to clear your name. And if it was a friend or family member that committed the crime, think very carefully before deciding to shield them.

## **Why Phishing Isn't Going Away**

---

There is no easy solution for phishing. There are ways to make it harder, which I explore throughout this book, but there's no true answer. Thieves go where the money is; right now, there's an awful lot of it accessible through the Internet. The Internet is still a new technology, and it's interfacing with older technologies—the banking and credit systems—that aren't prepared for the Information Age.

Still, the threat of being phished is not a reason to stop making financial transactions online. The same Internet that enables phishing also enables some of your best defenses against it, such as checking your accounts more frequently and ordering credit reports easily. Internet buying can save a lot of money and hassle. Savvy bidding on eBay can net you items that are simply not for sale anywhere, such as antique Pez dispensers. (eBay got its start as a way for Pez collectors to trade candy dispensers. Really.)

Many articles about phishing discuss how it's undermining customer confidence in e-commerce. It needn't. Given the number of different ways that your identity can be stolen, e-commerce is only a tiny bit more dangerous than regular commerce. This is especially true if you're reading this book—you're forewarned against the potential problems and will be on guard against the more dangerous schemes. Giving up Amazon or NewEgg.com isn't going to prevent a crooked employee at your bank/hospital/ISP/whatever from selling your information. Quitting online banking isn't going to stop your waitress from skimming your card at a restaurant.

Phishing is a real problem, but it's not a reason to hide from the Internet. So what do you do? Cultivate your inner smart alec so that you remain sufficiently skeptical of scams and schemes that come your way. Pay attention to what the latest frauds are. Don't engage in vigilante responses—this is unhelpful and often counterproductive. Write your congresscritters instead. Help educate your friends and family, especially those whose finances are combined with yours. If you want extra-good karma, help them with technical support. Watch your account balances. Do good, avoid evil, and patch your computer.

