Phishing Mongers and Posers

Unmasking deceptive schemes that range from clever to clumsy.

The following definition from the Antiphishing Web site (www.antiphishing.org) is a useful place to begin this column:

What is phishing and pharming? Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use 'spoofed' email to lead consumers to counterfeit Web sites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and Social Security numbers. Hijacking brand names of banks, e-retailers, and credit card companies, phishers often convince recipients to respond. Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using Trojan keylogger spyware. Pharming crimeware misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning."

The phish mongers to which I refer in the title of this column are those who deploy these phish scams in such a way that they stand a measurable chance of success against a reasonably intelligent and enlightened end user. The posers are the bottom feeders in the phishing community that exhibit a very low level of sophistication. This distinction is critical if one attempts to thwart phishing.

Phishing Facts

There's more to phishing than throwing digital bait on the Net. All too often descriptions of phishing scams drill down into deceptive URLs, fake address bars, and the like but fail to investigate the set-up that precedes the sting.

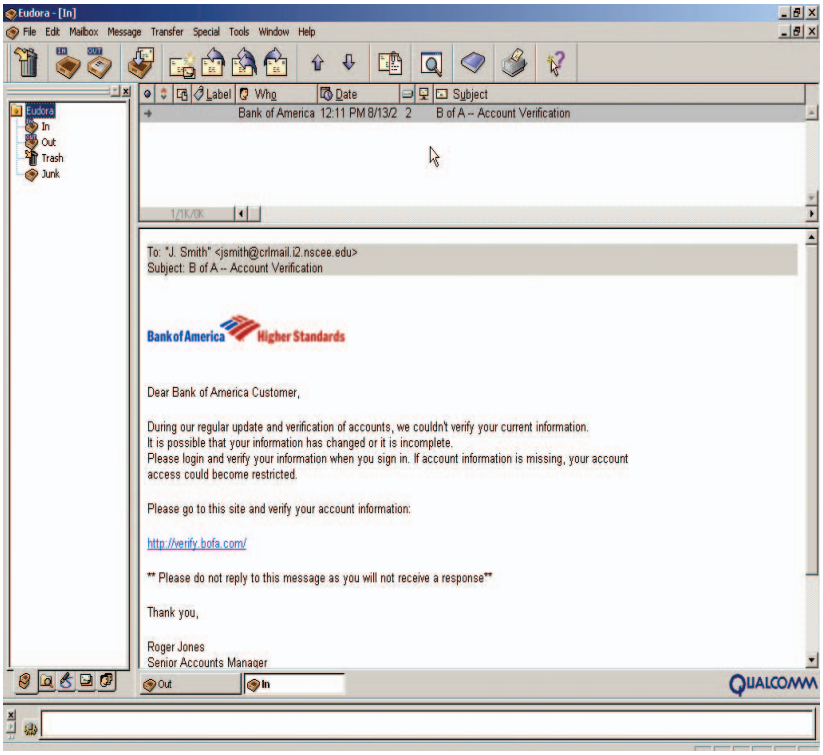
The essential requirements of effective phishing require the bait:

- Look real;
- Present itself to an appropriate target-of-opportunity;
- Satisfy the reasonableness condition (going after the bait is not an unreasonable thing to do);
- Cause the unwary to suspend any disbelief; and
- Clean up after the catch.

The similarities with angling should not be overlooked. There are reasons why anglers neither

ROBERT NEUBECKER

Figure 1a. Phishing email that satisfies the effectiveness criteria.



troll with charcoal briquettes nor fly-fish for sharks. I will illustrate the analogy to the digital surf with a few examples taken from one of the phishing research projects in our lab.

Figure 1a is modeled after some live phish we captured on the Net. Let's analyze this in terms of the five criteria listed earlier. First, the email looks legitimate—at least to the extent it betrays nothing suspicious to a typical bank customer (aka target-of-opportunity). The graphic appears to be a reasonable facsimile of a familiar logo, and the salutation and letter is what we might expect in this context.

Second, the target is the subset of recipients who are Bank of America customers. The fact that the majority of recipients are not customers is not a deterrent because there's no penalty for over-phishing in Internet waters. Third, the request seems entirely reasonable and appropriate given the justification. We reason that if we were a bank, we might do something similar under such circumstances. Fourth, the URL link seems to be appropriate to the brand. The unwary among us might readily trade off any lingering disbelief for the opportunity to correct what might be a simple error that could adversely affect use of a checking or credit card account. We may assume the link to verify.bofa.com would take us to an equally plausible Web form that would request an account name and password information.

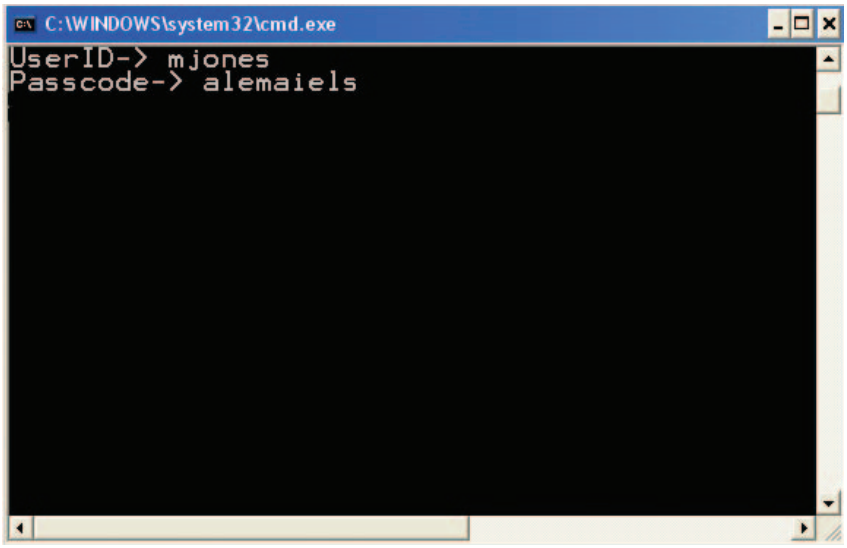


Figure 1b. Phishing from the phisherman's perspective.

The unwary in this case is M. Jones, whose harvested Web form appears to the phisherman as in Figure 1b. This is a screenshot of an actual phishing server in my research lab.

In order to complete the scam the fifth condition must apply. In

this case, after the private information is harvested, the circle is completed when the phishing server redirects the victim to the actual bank site. This has the effect of keeping the bank's server logs roughly in line in case someone makes an inquiry to the bank's help desk.

Figure 2 illustrates this activity. Of course, a more careful inspection of the bank's server logs would reveal a flaw in this simplified approach, because the phishing server shows up in as the "referrer"—a telltale sign the phisher would like to avoid. But, this deficiency could be overcome by a bit of careful packet crafting.

The preceding example is a well-known exploit strategy. Some sub-cerebral variations on this theme appear in the sidebar "Phishing Expeditions."

Mongers and Mayhem

So much for posers. My last example is a phish of a different stripe. So much so that it justifies discussion. It comes to us through an ISP in Shanghai in a cleverly disguised way.

Look carefully at the cursor in Figure 3. The cursor seems to be sensing the link even though it's not particularly close to it. The fact is it's not sensing that link at all, but rather an image map. A quick review of the source code, shown beneath the figure, leads us to a veritable cornucopia of trickery.

Several features make Figure 3 and its associated source code interesting. First, the image map coordinates take up pretty much the whole page. Second, the image that is mapped is the actual text of the email. So what appeared to be email was just a picture of email. Thus, the redirect was actually not a secure connection to eBay at all as it appeared, but an insecure connection to 218.1.XXX.YYY/

Phishing Expeditions

Example 1: from the 218.12. class B network registered to an ISP in Beijing.
GIST OF EMAIL: A U.S. bank admits that its database has been hacked. The bank needs to have your bank debit card number, account ID, and PIN immediately.
NOTABLE QUOTES: "This process is mandatory, and if you did [sic] not sign on within the nearest time [sic] your account may be subject to temporary suspension."
PHISHING LINE: http://218.12.29.40
TARGET-OF-OPPORTUNITY: Someone grammatically challenged, especially with respect to tense and adjectives, who both a fan of online banking and newbie to the Web.
EFFECTIVENESS CRITERIA SCORE: 0.5 out of 5.
Example 2: from the 80.53 class B registered to an ISP in Gdansk.
GIST OF EMAIL: An eCash service claims to have noticed attempts to log in to the user's account from a foreign IP address.
NOTABLE QUOTES: "...we have reasons to belive [sic] that your account was hijacked by a third party.... If you choose to ignore our request, you leave us no choise [sic] but to temporaly [sic] suspend your account."
PHISHINGLINE: click here
TARGET-OF-OPPORTUNITY: Submissive types who click on anything when told to do so and also subscribe to the school of relaxed orthography.
EFFECTIVENESS CRITERIA SCORE: 1 out of 5 is charitable.
EXAMPLE 3: from an IP in Russia operating through a Web hosting service in Jordan.
GIST OF EMAIL: A well-known Web auction company's Departament [sic] indicates that their records are out of date and that billing information must be updated within 24 hours or the account will be terminated.
NOTABLE QUOTES: "Departament" is just a start. How about "Please update your records in maximum 24 hours."
PHISHINGLINE: Please click here to update your billing records.
However, a look at the source page shows the actual URL is
<a href="http://darkcity.ru/acounts/memb/avncenter/dll87443/.BayISAPI.dll/hgdas676bsda6gwcv7zfcwfcwf34gfwf23g235f134f3fg3f&bhdfahva68532hbhwseBayISAPI.dllPaymentLanding&ssPageName=hhpayUSf&=userhgads&secure&ssl7r2vbd7d5b.html">. What is the likelihood that our auction company works under the domain name of "darkcity" through an ISP in Russia? I don't think so.
TARGET-OF-OPPORTUNITY: People who like lots of vowels who don't know how to use the "view source" menu option in their browser.
EFFECTIVENESS CRITERIA SCORE: 1.5 out of 5 seems generous to me.

If it weren't profitable for these cyber crooks to phish, they wouldn't do it.

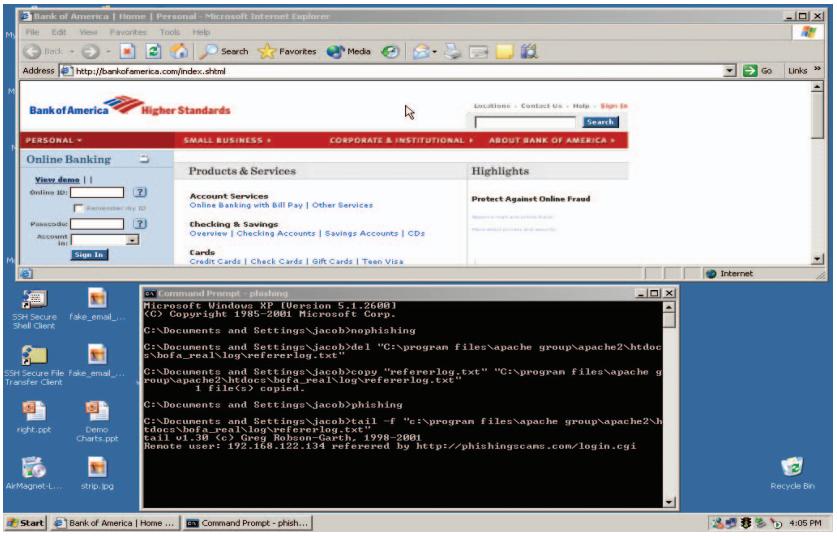


Figure 2. Phish clean up.

.../e3b/. While Windows users see the "dots of laziness" frequently when a path expression is too long for the path pane in some window, this isn't a Windows path in a path pane. These "dots of laziness" are a directory name. Now why would one create a directory named "…" It certainly falls short of the mnemonic requirements most of us learned in introductory programming courses.

On the other hand, it might blend in stealthily with the other Unix/Linux hidden files "." and ".." and possibly escape an onlooker's suspicion. This suggests the computer at the end of 218.1.XXX.YYY may not be the phisher at all, but another unsuspecting victim whose computer has been compromised (for that reason, I've concealed the final two octets of the IP address). Another sign of intrigue is the font color of almost pure white "#FFFFF3" for "Barbie Harley Davidson in 1803 in 1951 AVI." Though their names are sullied, neither Barbie nor Harley Davidson had anything to do with this scam. This white-on-white hidden text is there to throw off the Bayesian analyzers in spam filters. Note that the email text is actually a graphic, so the Baysian analysis likely concludes that this is about Barbie and her Harley.

As opposed to the posers, this phish monger is moderately clever. While the exploit may not earn a trophy, it's a keeper.

eBay®

Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information.

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply

Figure 3. Phish mongering.

Source Code for Figure 3

```
<x-html>
<html><p><font face= "Arial"><A
HREF="https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2
&siteid=0"><map name="xlhjiwb"><area coords= "0, 0, 646, 569" shape="rect" href=
"http://218.1.XXX.YYY/.../e3b/"></map><img SRC=
"cid:part1.04050500.04030901@support_id_314202457@ebay.com" border= "0" usemap=
"#xlhjiwb"></A></a></font></p><p><font color= "#FFFFF3">Barbie Harley
Davidson in 1803 in 1951 AVI
</x-html>
```

URL Pearls

The best starting point for phishing awareness is the Antiphishing Web site (www.antiphishing.org). This site contains useful statistics, charts, events lists, and archives of virtually all aspects of phishing collected by third-party sources. Not surprisingly, the site's bar charts reveal that phishing is on the rise. The statistics are unweighted so the impact of the major offending nations tend to be underrepresented. More meaningful measures might include percentages of attacks as a percentage of registered IP addresses, percentage of Internet traffic, and so forth.

Fraudwatch International's Web site (www.fraudwatchinternational.com) is a good place to start investigation of phishing scams. It lists current alerts for both phishing and non-phishing scams, Internet fraud, and identity theft. On a busy day, their Web site produces a dozen or more new phishing alerts. Since phishing is propagated primarily through email, the lifespan of a phish scam is measured in days before it is included in malware and firewall updates. Consequently, only the most recent reports represent those variations on the theme that are the most dangerous. As of this writing, there were 22,821 individual phishing exploits being monitored by Fraudwatch, 590 of which are currently active. Fraudwatch also offers Fraudshield, a phish-filtering utility that works much like an anti-virus program.

For a historical perspective on email, see my April 1997 column "Email: The Good, the Bad, and the Ugly."

Conclusion

It is unfortunate in the extreme that there are victims who fall for the fatuous phishing scams. We would all sleep better if the kind of flagrant errors characterized by our posers automatically ruled them out of all consideration. But they don't, unfortunately. Unlike cracking and the business of script kiddying, phishing is economically motivated: if it weren't profitable for these cyber crooks to phish, they wouldn't do it. And if the posers are occasionally effective, it's no wonder that the mongers account for economic losses in the billions of dollars each year—losses that are ultimately born by the customers.

All four examples, even those written by the posers, managed to escape detection by one of my spam/phish filters within the last few months. The likelihood is that future phishing, or whatever phoolware follows it, will continue the cat-and-mouse game with security software. Perhaps our greatest mistake is excessive reliance on technology solutions. Our efforts seem no more effective at blocking phish scams now than they were at blocking embedded executables 10 years ago.

When it comes to email, common sense still goes a long way. C

Hal Berghel (www.berghel.net) is associate dean of the Howard R. Hughes College of Engineering and Director of the Center for Cybermedia Research at the University of Nevada, Las Vegas, and co-director of the Identity Theft and Financial Fraud Research and Operations Center.

THE HISTORY OF ACM

As the 60th anniversary of ACM approaches, *Communications* is planning a special section next year on the history of the organization, its activities, and its role in the development of computing. The guest editors of this section are particularly interested in articles from historians of computing.

Articles should be about 3,000 words in length and should be submitted to David S. Wise (dswise@cs.indiana.edu) by May 16, 2006. Authors will be notified of a preliminary decision in October 2006 and will have until December 15 to submit a revised version for final consideration.