

The Dumbing Down of SportPhishing

Hal Berghel
 University of Nevada, Las Vegas



The current crop of phisherpersons can't see the phorest phor the phurze.

Legend has it that the first description of the phishing technique dates back to a 1987 presentation at an Interex conference by Jerry Felix and Chris Hauck ("System Security: A Hacker's Perspective"; (www.peterjbentley.com/bibliography.pdf). Within 10 years, the technique was informally named phishing ([www.brighthub.com/internet/security-](http://www.brighthub.com/internet/security-privacy/articles/82116.aspx)

[privacy/articles/82116.aspx](http://www.brighthub.com/internet/security-privacy/articles/82116.aspx)). That was eons ago in IT years—plenty of time to evolve into new and mysterious techniques. So why is it that we're still trolling for the bottom feeders of the phishing world?

PUTTING IT IN PERSPECTIVE

Let's put this in perspective. In 1987, Microsoft had just released Windows 2.0 as its latest "killer" DOS shell. The newest Intel CPU offering

was the 386. Morris hadn't launched his worm yet. The number one song on some charts was Ben E. King's "Stand by Me." The big TV premiere of the year was *Married with Children* on the new Fox network, and *Seinfeld* was still a dream for Jerry.

We're talking a long time ago. And after all that time, we're just now seeing the last of the Nigerian 419 scam. Where is all the e-criminal talent? We seem to be regressing here.

I offer the following modest examples in support of this claim. Let's begin with the cryptic phish bait in Figure 1. Clearly, this minimalist offering is motivated by some serious cyber-illiteracy. Even on the face of it, this is a paradigm case of "phatuous phish bait":

- the user-defined return e-mail address domain name is uninformative;
- the return e-mail address doesn't match the sender's name;
- the e-mail is forwarded;
- the target is unnamed;
- the message is evasive and obscure; and
- the filename of the attachment = <Details.zip>.

But that's only the surface. Perusal of the e-mail header in Figure 1b reveals the following:

First off, the e-mail source (186.113.217.18) is assigned to an ISP

Re: Fwd: Wire Transfer Confirmation (FED 84788AN662)
 GABRIELLA PEREZ <YareliGierling@ptd.net>
 Sent: Tue 7/3/2012 4:10 AM
 To: Hal Berghel
 Message Details.zip (62 KB)

Dear Operator,

WIRE N: FED-406812546223382

STATUS: REJECTED

You can find details in the attached file.

(a)

Received by: (Postfix) id 4FDB9C73EB; Tue, 3 Jul 2012 06:29:46 -0400 (EDT)
 Delivered to:
 Received: from [186.113.217.18] (unknown [186.113.217.18])
 Received: from [186.113.217.18] by smtpin.ptd.net; Tue, 3 Jul 2012 06:10:19-0500
 Message-ID <B6796796E5B6796EC8BD3EC8B6710109@AWDn>
 From: GABRIELLA PEREZ <YareliGierling@ptd.net>
 Subject: Re: Fwd: Wire Transfer Confirmation (FED 84788AN662)
 Date: Tue, 3 Jul 2012 06:10:19-0500

(b)

Figure 1. Phish bait examples: (a) cryptic phish bait and (b) a bogus e-mail header.

in Columbia, while the registrar of record for ptd.net is the Internet support service, Tucows.com, a company that is far too big to cooperate with Columbian ISPs on phishing scams. Predictably, an e-mail validation test on YareliGierling@ptd.net yields a 550 error: Sorry, no mailbox by that name <reset>.

There's nothing about this e-mail that even pretends to ring true—either on the surface or based on an analysis of the header. C'mon, Gabriella, Yareli, or whoever you are. This is a really lame effort. Read a book.

I next offer Figure 2 for your consideration. I've received literally hundreds of these bogus UPS notifications in the past few months—I'm about to drown in digital brown at this point.

Note that the target of this absurdity is {mailto_username}@{mailto_domain}. C'mon script kiddies, learn about the operation of scripting variables before you use them. Note also that the tracking number link to the malware that starts the infection cycle is startupwordpresstoday.com/spss.html. What is the chance that UPS will store this tracking number database on startupwordpresstoday.com, which, incidentally, is registered to a Houston P.O. box of a bogus Hotmail account holder? Call me crazy, but I have a hunch that UPS doesn't use hotmail account holders as its registrars of record.

As an aside, all links on the page but the last point to the same malware—a technique that, for want of a better term, I'll call phishing by "snaglining." By the time this subcerebral phishing effort reached me, the DNS records had already been pulled, and the domain name appeared on several blacklists.

Consider the Bulgarian contribution in Figure 3. Although the phish bait came from Sofia, the link reveals that the server that plants the malware is a legitimate automobile dealer in Canada. While the bait itself has

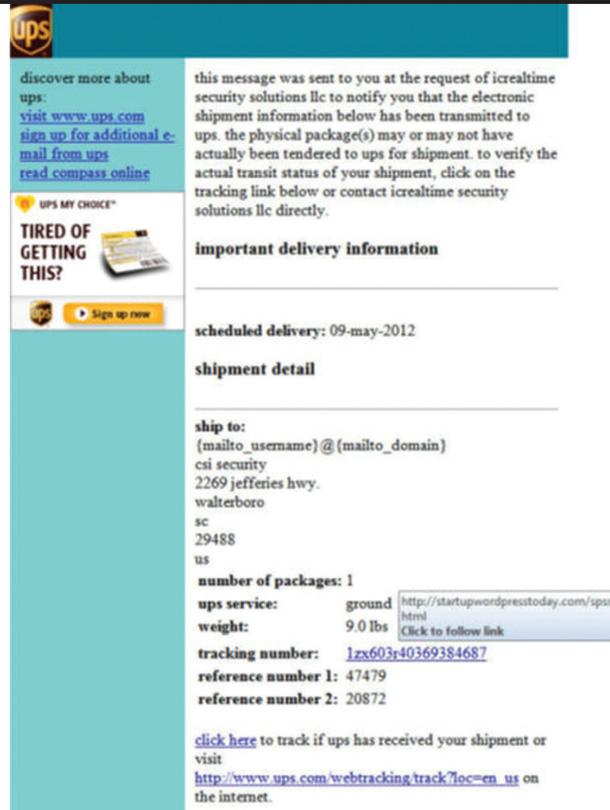


Figure 2. Spray-n-pray with "snaglining."



Figure 3: Chevrolet phishing tackle.

The screenshot shows an eBay phishing email. The email body contains the eBay logo, a greeting 'Dear eBay Member', and a message stating that the account could be suspended for not updating account information. It provides a URL: https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0. It also includes a warning about account suspension and a reference to the User Agreement. The HTML source code (b) shows a classic phishing technique: a map with a hidden area containing a link to the same URL as in the email body, and an image with a white border and text 'Barbie Harley Davidson in 1803 in 1951 AVI'.

Figure 4. Phish bait with pedagogical value: (a) classic example, circa 2005, and (b) HTML version.

little going for it, the person who hacked into the automobile dealer's server scores higher marks for skill.

By the time the e-mail reached me, some attentive IT person had removed the malware executable from the car dealer's website—that's a good thing—but the hacker's directory

structure was left intact, presumably for further investigation.

CURRENT PHISH BAIT STINKS

For the most part, current phish bait stinks. It's too brutish and lacks any semblance of creativity or sophistication. This displays a serious

dumbing down of phishing generally, which now seems to be almost exclusively in the hands of unenlightened script kiddies. This wasn't always the case. Five to 10 years ago, I received a continuous stream of grist for my network forensics students' lab assignments. The latest offerings are too low-brow even for neophyte students.

To illustrate, consider the old-school classic phish bait in Figure 4. This is bait that serious undergraduates can get their hands around. Note the creative use of an image map with a nonmnemonic filename as the link's anchor, the stealthy Unix subdirectory name (...) to avoid the computer owner's suspicion, and the gratuitous hidden text (white on white) to fool e-mail software's Bayesian analyzer. This is phish bait with pedagogical value, unlike its unworthy successors.

Whatever happened to the skillful hackers of yore who gave the world techniques like those in Figure 4—as well as script embedding, domain and URL spoofing, ASCII character convolutions, and Unicode/escape encoding? Few ever got prosecuted, much less convicted. This lost generation of phishers left an e-crime void that has been filled by merchants of mediocrity. **C**

Hal Berghel, Out of Band column editor, is a professor of computer science at the University of Nevada, Las Vegas, where he is the director of the Identity Theft and Financial Fraud Research and Operations Center (itffroc.org). Contact him at hlb@berghel.net.

THE OUT-OF-BAND ANNUAL SPORTPHISHING TOURNAMENT: CALL FOR NOMINATIONS

Get your phish groove on by participating in the new Out-of-Band SportPhisher of the Year Tournament for the best and worst phish bait of the year.

Send me a screenshot of the phishbait along with justification for why you think your candidate is a winner (or loser). Hang on to the actual e-mail, as I'll request it from the finalists for analysis. If your entry is selected, you'll be credited for the submission (or you can retain anonymity—your call).

Send your tournament entry to me at hlb@computer.org by **1 November 2012**.

cn Selected CS articles and columns are available for free at <http://ComputingNow.computer.org>.