An Analysis of a "Phishing" Expedition

By Rick Hellewell
www.digitalchoke.com/daynotes
December 20, 2004

If you have an email address, you will get a 'phish' email. This is a term for an email message that directs you to a web page that will ask for your financial information: your credit card number, PIN code, mother's maiden name, social security number, etc. The message will tell you that some account has to be verified. It may be your bank, your credit card, or eBay or PayPal. There are a lot of phishing emails, some experts think that phishing is going to be more common in 2005. One source for information, along with an archive of examples, is the Anti-Phishing Working Group, at www.anti-phishing.org .

Phishing is an example of the 'social engineering' hacking technique. One famous social engineer is Kevin Mitnick, who describes various examples in his book "The Art of Deception". You gain the trust of a victim (by sending out an authentic-looking email) and then abuse that trust for personal gain (by 'harvesting' their financial information via a web form).

Dr. Pournelle has a very visible email address; it's published in his web "Daynotes" pages and many other public/web forums. Email addresses are very easily harvested using techniques similar to how Google indexes web pages. There are programs available in the hacker world that will crawl the internet, extracting email addresses where they are found. It will find an email address in the HTML code similar to "mailto:yourname@yoursite.com". Or, you can just buy a million email addresses for under US$100.

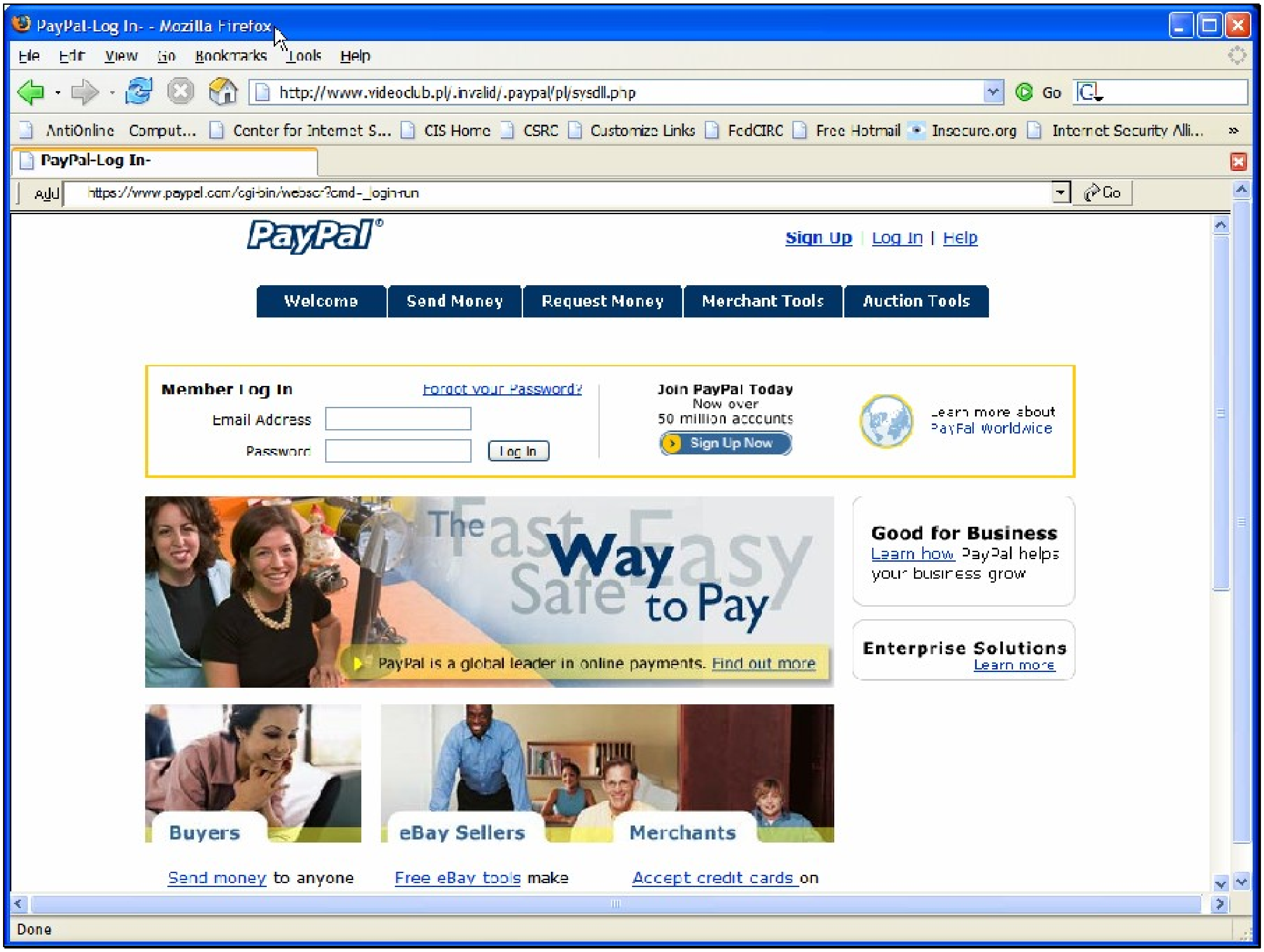
The email Dr. Pournelle received contained text indicating that he had added a new email address to his PayPal account. On first glance, the message looks to be authentic. There are no obvious spelling or grammar errors, and there are links to the PayPal site. There are more sophisticated phishing emails; many will have the 'look and feel' of the targeted site, with actual graphics.

The intent is to get you to click on the link, which will take you to the PayPal site where you can verify your information. Except it's not PayPal that is your destination, it is the phisher's site that has been built to look like PayPal's site.

This particular phish had some interesting and commonly used techniques. The message's visible link says https://www.paypal.com , but the actual code "under" the link directs you to a site in Poland called "videoclub". Although it is possible that that site has been hacked to provide the phishing code, the content of the videoclub site appears to be pirated movies. The site is not English; I am assuming Polish language, but there is what appears to be an offer for the "Ocean's 12" movie.

Being a brave sort (and with my firewall and anti-virus protection firmly in place), I went on a short phishing tour via the link in Dr. Pournelle's email message. (Please don't try this at home without proper precautions. If you are interested in other examples, go to the Anti-Phishing Working Group site.) I also used some text-based tools to get the pages without displaying them in a browser.

The first stop on my phishing tour was a welcome to "PayPal" (see figure).


PayPal-Log In- - Mozilla Firefox

http://www.videoclub.pl/.invalid/.paypal/pl/sysdll.php

Addr https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

Member Log In

Email Address

Password

Join PayPal Today
Now over
50 million accounts

Learn more about PayPal Worldwide

Good for Business
Learn how PayPal helps your business grow

Enterprise Solutions
Learn more

PayPal is a global leader in online payments. Find out more

Send money to anyone

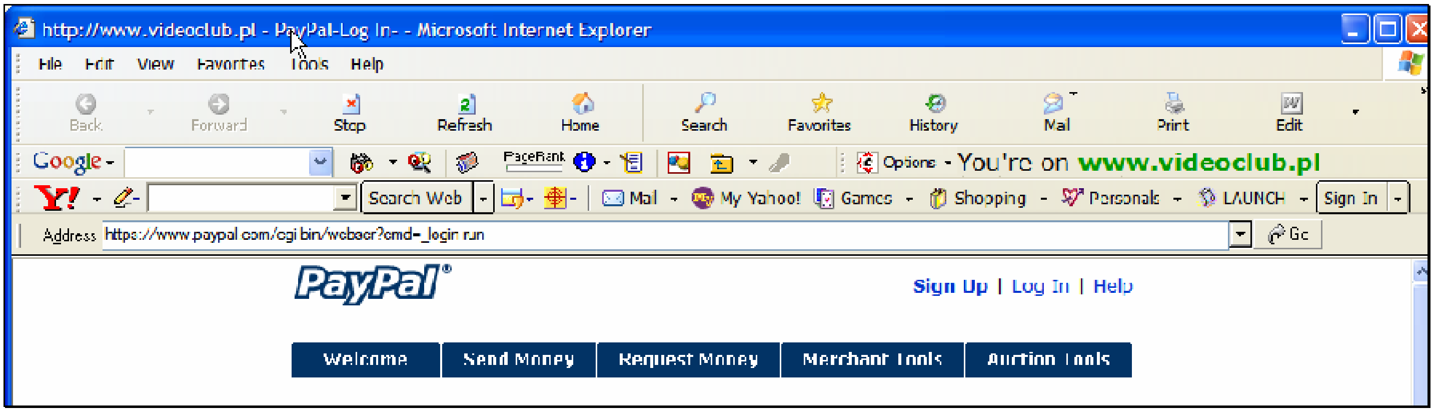
Free eBay tools make

Accept credit cards on

If you just look at the visual area of the page, you can see that the "look" of the page is very similar to what you would see at the actual PayPal site. There are official logos, and nice pictures of smiling people, and the "member login" area. There are links to get more information, or even to sign up for a new account. It looks just like a PayPal site.

There are some problems, though. Each of the links goes to the same login page of the phisher's web site. No matter what link you click on, you'll get to the login page. If you click on the "join" icon, you'll eventually get to a page that will look just like PayPal asking you for your financial information. Each of the pages will look like the actual PayPal site. (And in fact, it is very close – the fake PayPal site looks just like the home page at www.paypal.com . Compare for yourself.)

If you take a closer look at the above screen shot, you will see some interesting things. Notice just above the page window area is a line with an "Address" bar showing a PayPal address. That address bar is actually part of the HTML code in the phisher page. It uses a technique to build its own browser window without the normal address bar, and places a graphic of the fake address bar over the usual location. The above screen is the link as shown in the FireFox browser. The following figure is how it looks in my fully patched Microsoft Explorer window (just the top part of the screen), but with some additional add-ins I use that are not in the standard IE installation.


http://www.videoclub.pl - PayPal-Log In- - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit
Google PageRank Options You're on www.videoclub.pl
Y! Search Web Mail My Yahoo! Games Shopping Personals LAUNCH Sign In
Address
Go
PayPal®
Sign Up | Log In | Help
Welcome Send Money Request Money Merchant Tools Auction Tools

Address https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

Notice that the “Address” bar is showing that you are on the PayPal site. Now my IE browser is a bit different than most. I’ve got the Google and Yahoo search toolbars, and that “You’re on..” area to the right. That is a browser add-in called “SpoofStick” (available at www.spoofstick.com, in IE and FireFox versions). It will show you the actual site you are looking at; in this case, the “Videoclub” site. If you have a standard installation of IE or FireFox, it will look like the above without the Google and Yahoo toolbar rows of icons. The “Address Bar” will show what looks to be a valid PayPal link.

The technique of displaying a bogus address bar is fairly simple. First, you use some common JavaScript to create a new full-screen browser window without the address bar. You also don’t display the minimize or maximize buttons, so that the page can’t be resized – that would make the address bar look wrong.

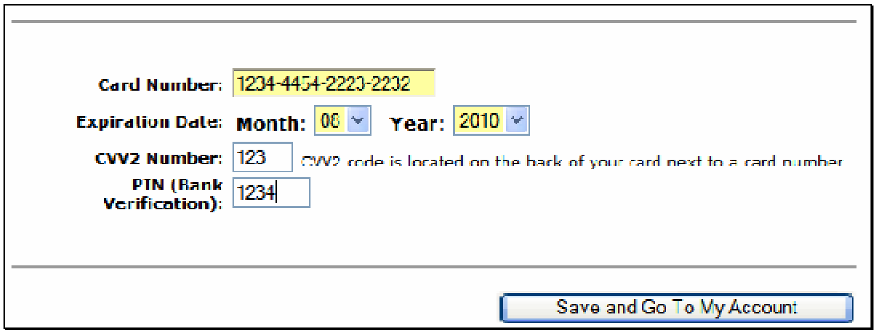
Then put in some browser checking code. Depending on the browser, position the address bar properly. If the browser is not supported, then redirect to the real PayPal page. This ‘intelligence’ is becoming more common; I found some basic information about this technique that was dated April 2004. The page code for the phishing pages seems to have been refined to include other browsers, although (as you can see from the IE and FireFox screen shots above) the address bar positioning is not quite perfect in non-IE browsers.

So the phisher’s technique of faking the address bar is mainly built for people using IE. That stands to reason, since IE is widely used. A phisher will use techniques to fool the 90% of people that use IE. (I suspect that as alternative browsers become more popular, the phishers will adapt their techniques to those browsers.) FireFox puts their address bar in a slightly different location, so this technique doesn’t work as well in FireFox as it does in IE, as you can see by the first figure.

But many people won’t look at the address bar, and they certainly don’t have something like SpoofStick (although it is recommended). They will just look at the web page content, see that it looks OK, and happily click on the links to take care of their problem. If you aren’t paying attention to the address bar, any browser will do for this phishing trip – even FireFox.

Continuing to throw caution to the wind, and because it’s a quiet day here, I did some “happy clicking” of my own. What I found was typical of phishing sites – the phishers are trolling for financial information.

The next screen I got was one that tells me that “PayPal” needs to verify my identity. This page is a form that asks for my credit card number, expiration date, CVV2 code, and PIN number (next figure; this and subsequent figures are cropped for space, but the original pages continue to show that PayPal “look”).



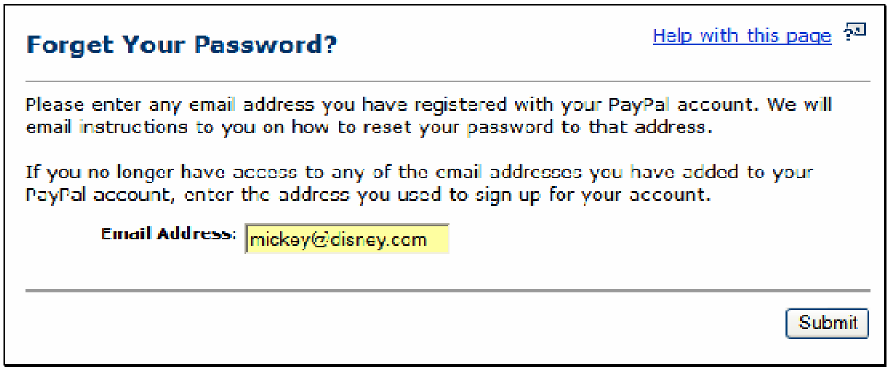
Card Number: 1234-4454-2223-2232

Expiration Date: Month: 06 Year: 2010

CVV2 Number: 123 CVV2 code is located on the back of your card next to a card number

PIN (Bank Verification): 1234

So I entered some fake information, and clicked on the “save” button. This site doesn’t do any verification for a valid credit card number (although that verification could be easily added). But the phisher decides that as long as I am giving out my credit card number, they might as well ask for more information. So the next screen asks for my email address (probably so they can send out more phishing emails; valid email addresses are also more valuable to sell to other spammers):



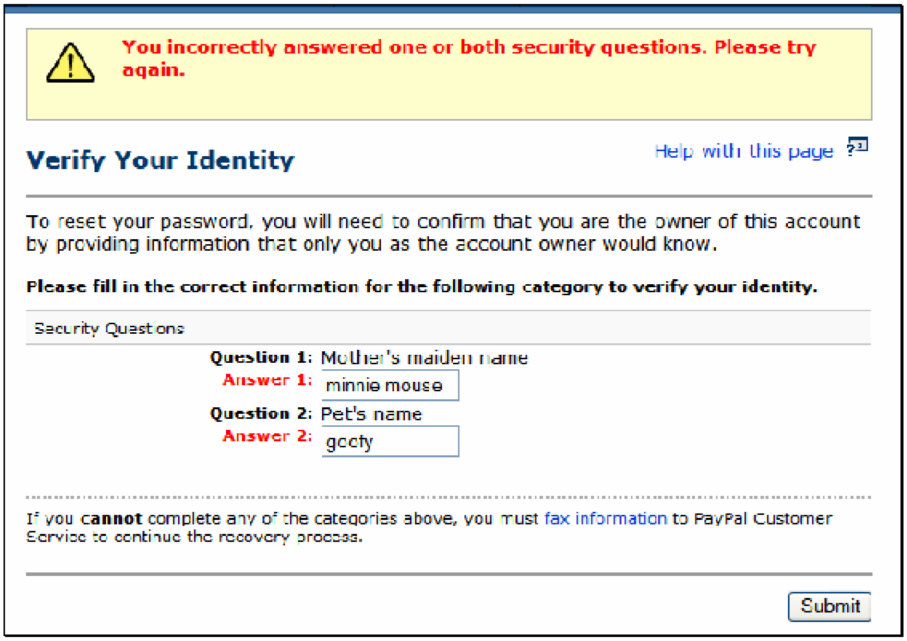
Forget Your Password?

Please enter any email address you have registered with your PayPal account. We will email instructions to you on how to reset your password to that address.

If you no longer have access to any of the email addresses you have added to your PayPal account, enter the address you used to sign up for your account.

Email Address: mickey@disney.com

Just in case that email address is not valid, the next screen has a spot to click on a link if “I no longer have access to this email address”. That link takes me to another place where I can continue to verify my identity, asking for my mother’s maiden name, and my pet’s name. Again, I enter bogus information, and I get this screen telling me that my answers were incorrect:



You incorrectly answered one or both security questions. Please try again.

Verify Your Identity

To reset your password, you will need to confirm that you are the owner of this account by providing information that only you as the account owner would know.

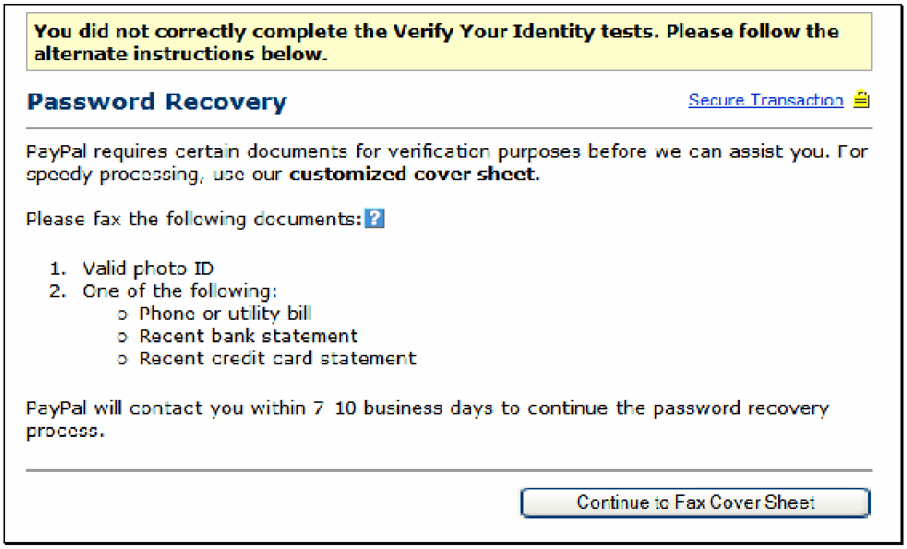
Please fill in the correct information for the following category to verify your identity.

Security Questions

Question 1: Mother's maiden name
Answer 1: minnie mouse
Question 2: Pet's name
Answer 2: goofy

If you **cannot** complete any of the categories above, you must fax information to PayPal Customer Service to continue the recovery process.

Another slightly clever technique used by the phisher: claim that the information is incorrect, and ask again to get different answers that might be useful. I try a few more invalid entries, and get to this official looking screen where I can gather some more information to send via fax:



You did not correctly complete the Verify Your Identity tests. Please follow the alternate instructions below.

Password Recovery

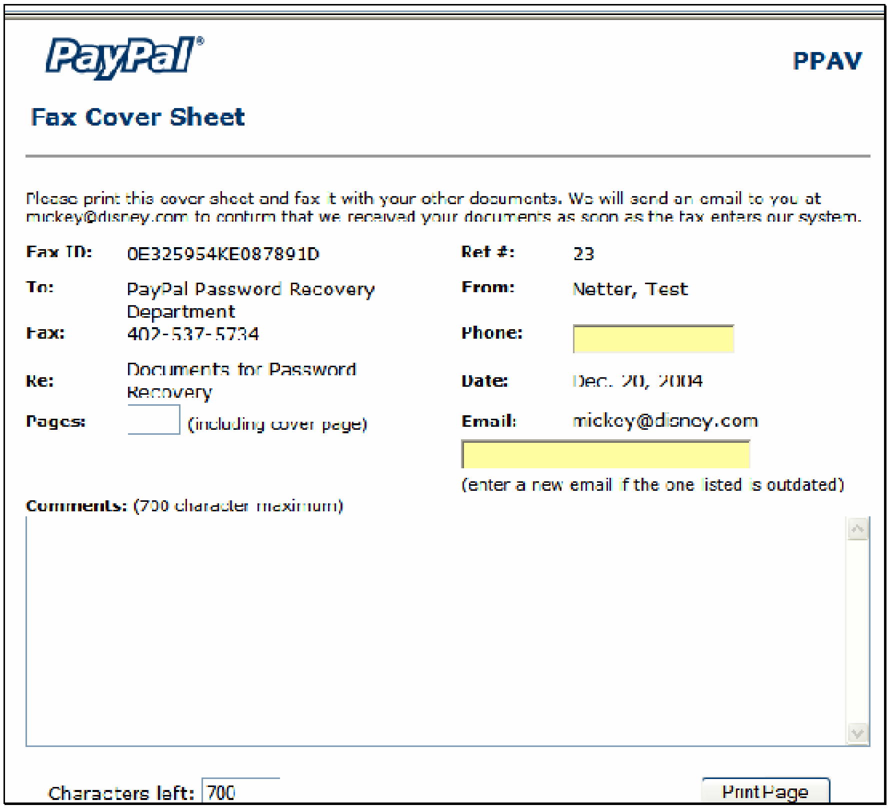
PayPal requires certain documents for verification purposes before we can assist you. For speedy processing, use our **customized cover sheet.**

Please fax the following documents:

1. Valid photo ID
2. One of the following:
   - Phone or utility bill
   - Recent bank statement
   - Recent credit card statement

PayPal will contact you within 7-10 business days to continue the password recovery process.

All I need to do now is to fax a copy of my utility bill (good for my street address), and my bank or credit card statement (more good information). And I can conveniently use their “customized cover sheet”, which looks like the next figure.



Fax Cover Sheet

Please print this cover sheet and fax it with your other documents. We will send an email to you at mickey@disney.com to confirm that we received your documents as soon as the fax enters our system.

Fax ID:	0E325954KE087891D	**Ref #:**	23
To:	PayPal Password Recovery Department	**From:**	Netter, Test
Fax:	402-537-5734	**Phone:**	
Re:	Documents for Password Recovery	**Date:**	Dec. 20, 2004
Pages:	(including cover page)	**Email:**	mickey@disney.com
			(enter a new email if the one listed is outdated)

Comments: (700 character maximum)

Characters left: 700

There is more to this page than shown in the screen shot; the bottom of the page has a nice bar code, for tracking purposes, I guess.

At this point, I quit. I haven’t tried the phone number. It’s in the 402 area code, which corresponds to somewhere in Nebraska (USA). That phone number may even belong to PayPal. (I’ll bet that one of Dr. Pournelle’s readers will provide information about that phone number.) But at this point, the phisher doesn’t really care who gets the fax. They have all the information they need to start charging the credit card account.

--oo—

These types of phishing techniques are commonly used. By sending a valid-looking email, and taking the time to build an authentic-looking site, the phisher can easily gather financial information. If they send out a million emails (not that hard), and only get a .005% response rate, they will have information for 500 accounts. Set up some quick charges of US$500 each and you have got a quick US$250,000 return. That's just for **one** phishing email, and that low response rate is easy to get. Not a bad return on your investment.

Phishing is a social engineering attack. It's not preventable by anti-virus settings, firewalls, or other computer security. It isn't prevented by the browser that you use.

Successful phishing depends on the lack of security between your ears. It's a user-education problem. If you are reading this on Dr. Pournelle's web site (or my site at www.digitalchoke.com/daynotes), we can assume that you are cognizant of these types of attacks. But even the "semi-geeky' can be fooled by some clever social engineering (Kevin Mitnick's book is full of such examples, even though many of his examples are dated).

You might think about putting a "pause" button between your finger and the mouse. Don't be too quick to click on a link. If you think the email is valid, then type in the address in your browser, don't click it. And even then, stop and think a bit.

--oo--

Current document version is located at www.digitalchoke.com/daynotes . Please use that link if you wish to share this with others.

-30-