With so much attention being paid to Phishing lately it would be a good idea to spend our May, Technology Security & Privacy News, article on the subject. For the record WIU has had twenty one (21) Phishing incidents resulting in thirty four (34) passwords resets as a result of someone responding to an email scam during the first four months of 2008 (for an average of 5.25 Phishing incidents and 8.5 related password resets per month or 1.6 password resets on average per Phishing incident). We do not have historical data to determine if these numbers are high, average or low. I can tell you that worldwide tracking of Phishing incidents puts the average at over 25,000 Phishing incidents per month (higher education specific numbers are not maintained). In the following article I will endeavor to put Phishing in to historical perspective and hopefully share some awareness along the way.

Phreaking, SPAM, Phishing, Botnets, Pharming, Vishing, SMiShing & SPIM oh my

It began in the 1950s with mostly kids & young adults making free phone calls by experimenting with telecommunications equipment also known as Phreaking (depicted in the 1983 movie *WarGames* starring a very young Matthew Broderick). The intent like all hacking in those days was more about the intellectual challenge. The victim was the big bad phone company. The subculture was in many ways glorified.

As the subculture matured in the 1980s, the tone began to change from one of curiosity to one of contempt mostly against the big software companies for putting out shabby unsecure code. The average computer user was seen as a pawn useful in making their point. To carry out their campaign they needed to infect computers with malware in mass quantity. SPAM or the mass broadcasting of email messages was the perfect vehicle. For this to work they needed to trick you in to clicking on infected email attachments. So we in the Internet security business began our own “do not click on unsolicited attachments” campaign.

The 1980s was also the beginning of the mass market appeal of the World Wide Web (WWW). With it came an evolution in the ability to infect mass amounts of computers. By sending SPAM crafted to look like a legitimate request from say your bank or university, you could be tricked in to following a link to a web site that was hosting malware. This in fact could have the same results as you clicking on an infected email attachment. Once again we in the Internet security business began our own “do not follow unsolicited web links” campaign.

The subculture changed again in the 1990s towards a drive for financial gain. Using the same basic technique, of sending out email SPAM crafted to look like it was sent by a legitimate institution and thereby tricking you to follow a link to a web site that had been crafted to also look like it belonged to a legitimate institution, you could be tricked in to divulging personal information about yourself (a technique known as Phishing). This technique uses email SPAM to cast a wide net (using a fishing metaphor) but a variant on this approach uses just enough information about the victim gathered from other sources (such as going through your garbage for unshredded documents also known as dumpster diving) to in act a much more personalized attack (know as Spear Phishing for its targeted victims). Spear Phishing attacks that target corporate "big fish" have been referred to as "whaling."

The reward was twofold. A perpetrator could go after whatever financial resources you had such as your bank account, credit or debit card, etc (know as financial fraud) or they could capture enough information about you to take over your identity (known as identity theft). Identity theft potentially being even more devastating to the victim because a perpetrator could use your identity to open up accounts, credit & debit cards and even commit other crimes hidden behind your identity (stuff that could potentially follow you throughout life). According to the FTC, in 2006 there were over 670,000 consumer fraud and identity theft complaints in the United States (29% of those involving victims between the ages of 18 29 and 5% involving younger victims).

The turn of the century saw the entry of organized crime and foreign governments in to the mix. It also saw the development of an international black market for the sale and purchase of everything from malware, stolen

credit/debit cards, SSNs, entire identities to do it yourself Phishing kits. Something else available for international sale or rent is control over compromised computers (typically as one of many compromised computers known as a Botnet). This could give the perpetrator the ability to hide behind your computer giving the impression that you are the perpetrator and not just a victim.

A disturbing trend is to use the Internets naming system also called DNS (Domain Name System) to obscure the perpetrator behind a botnet load of victims. Changing between compromised computers to make it look like an ever changing list of computers are doing the SPAMing (this use of DNS for Phishing is called fast-flux or Rock Phishing after the criminal gang that made it famous). This makes it difficult for law enforcement to take down the true perpetrator (also called the command & control center) as it appears to be a moving target. A technique called Pharming uses DNS cache poisoning to redirect you to a malware hosting web site without you having clicked on any link. This advance attack typically will involve modifying a local DNS file on a compromised computer or compromising a DNS server that will be handing out incorrect DNS entries when legitimate web sites are requested. For example, if I can compromise a DNS server and have it give out information about my malicious web site instead of say myspace.com, facebook.com, youtube.com or www.wiu.edu you can begin to see why folks in my line of work are sleep deprived.

So how do we deal with all of this? Well I say if someone asks you for personal information chances are the request is not legitimate. After all, your school, bank, credit union, Credit Card Company, Phone Company, library, church, etc. rarely if ever will send you unsolicited requests for personal information. A pretty good rule of thumb is: verify the source before providing any personal information and challenge the request if in your mind the amount of personal information requested appears excessive. After all your personal business is your business and your personal data is your data. Why would you not be skeptical when it comes to your personal information? Now if I could only make this in to a campaign slogan.

One additional thing you can do to protect yourself from Phishing is to use the latest version of your favorite web browser. Internet Explorer 7 and Firefox 2 have built-in anti-phishing technology that alerts you when you browse a reported Phishing site (no such technology is currently part of the Mac OS Safari browser).

What comes next? One could expect Phishing attacks to expand to use other technologies such as cell phones, text messaging, etc. After all we already have names ready to use such as SPIM (SPAM over IM), SMiShing (Phishing using SMS text messaging) & Vishing (Phishing using VOIP).

FYI: With most students & faculty being away for the summer, this newsletter will take the summer off as well and return in September. Have a safe physical & virtual summer!

Best Regards,

Michael Rodriguez
CTSO @ Western Illinois University
ma-rodriguez2@wiu.edu

"Let us not look back in anger or forward in fear, but around in awareness." - James Thurber