Global Information Assurance Certification Paper

If you build it, they will come: A Look into Phishing Attacks

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4b

Option 1- Research on Topics in Information Security

Submitted by: Todd Johnson
Location: SANS Denver

Abstract

E-commerce as we know it is under attack. Customer confidence is wavering. Personal information is being stolen by "phishers" and new attacks occur almost weekly. There seems to be no end in sight to this problem. The only real solutions in the war against online fraud, also know as phishing, are a combination of multi- tiered business solutions and more importantly, user education.

You receive an email from Mybank.com, *"For security purposes, your account has been randomly chosen for verification. To verify your account information, simply provide us with the requested data."* For those of us with a good amount of experience in online business, this may sound a bit fishy, so we're likely to ignore and delete it. But, to someone less experienced, this may sound like a legitimate request. That is exactly what the "phishers" are counting on.

"Phishing (sometime called carding or brand spoofing) is a scam where the perpetrator sends out legitimate- looking emails appearing to come from some of the web's biggest sites, including EBay, Pay Pal, MSN, Yahoo, Best Buy and America Online, in an effort to phish (pronounced "fish") for personal and financial information from the recipient".[1] Phishers like those who bombard our email boxes with spam, are well aware that most people will see their emails as junk and discard them. And just like spammers, phishers are counting on the small percentage of users to believe the email, to execute their scam. "Whereas all spam is not a scam, all attempts at phishing are scams".[2] According to the Anti-Phishing Group (www.Antiphishing.org), "data suggests that phishers are able to convince up to 5% of recipients to respond to them."[3] Large scale phishing attacks were first reported in November and December of 2003, when Citibank customers were targeted. The Anti-Phishing Group (APWG) noted that the number of unique phishing attacks nearly tripled between March and April of 2004. During the month of March 402 unique attacks were reported. During the month of April the number of unique attacks rose to 1125.

According to the Gartner Group (www.Gartner.com), provider of research and analysis for the IT industry, 57 million Americans reported to have received some form of phishing email. Of them, 11 million admit to having clicked on a link embedded within the email. And 1.8 million admit to having been fooled into giving away personal information. "The research company [Gartner] said that crimes such as phishing, whereby criminals use misleading emails and Web sites to dupe individuals into sharing personal data like passwords, accounted for a staggering $2.4 billion in fraud, or an average of $1,200 per victim, during the last 12 months".[4]

Before we can look into prevention and other solutions to phishing, we need to look into the make up of a phishing scam. There are many types of phishing scams. The techniques being used are as simple as a poorly written email, to ones that imitate viruses. Some of the earliest phishing scams originated in non- English speaking countries, they were easy to detect and avoid, because of the poor grammar and many spelling errors.
From a high level perspective, all phishing scams can be categorized into two main parts; a hoax e-mail and a hoax web page. These parts tend to be used

---

[1] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci916037, 00.html
[2] http://techupdate.zdnet.com/techupdate/stories.main/Phishing_Spam_that_can't_be_ignored.htm
[3] http://www.AntiPhishing.org
[4] http://zdnet.com.com/2102-1105_2-5234155.html? Tag= print this

together, although with a cleverly written Java Script, that briefly redirects a victim and download a key logger or Trojan, victims can have personal information stolen, without ever receiving an email or clicking on a web link.

Hoax E-mail

For your chance to win a new car click here
For a free dinner at {insert restaurant here}, just fill out this survey
For account verification purposes, please log into your hotmail account

The simplest phishing attack is one in which, a victim receives an email, requesting personal information. Those who tend to respond believe they have been singled out to receive the special offer or request. One of the best known examples of this type of scam has come to be known as the "Nigerian 4-1-9 scam". The email is supposed to be from a member of a government contract review panel in Nigeria. The deal is, there are millions of dollars trapped in a bank account, and they need an account outside of Nigeria, to transfer the funds. Once a bank account has been found, the money will be transferred, with the owner of the account keeping 20% of the transferred amount. The remaining 80% will released to the government contract review panel.

The "Nigerian 4-1-9 scam" was named for the Nigerian penal code for this type of fraud. The email itself has taken many forms over the years, but in general it looks something like this:

REQUEST FOR URGENT BUSINESS RELATIONSHIP
FIRST, I MUST SOLICIT YOUR STRICTEST CONFIDENCE IN THIS TRANSACTION. THIS IS BY VIRTUE OF ITS NATURE AS BEING UTTERLY CONFIDENTIAL AND 'TOP SECRET'. I AM SURE AND HAVE CONFIDENCE OF YOUR ABILITY AND RELIABILITY TO PROSECUTE A TRANSACTION OF THIS GREAT MAGNITUDE INVOLVING A PENDING TRANSACTION REQUIRING MAXIIMUM CONFIDENCE.

WE ARE TOP OFFICIAL OF THE FEDERAL GOVERNMENT CONTRACT REVIEW PANEL WHO ARE INTERESTED IN IMPORATION OF GOODS INTO OUR COUNTRY WITH FUNDS WHICH ARE PRESENTLY TRAPPED IN NIGERIA. IN ORDER TO COMMENCE THIS BUSINESS WE SOLICIT YOUR ASSISTANCE TO ENABLE US TRANSFER INTO YOUR ACCOUNT THE SAID TRAPPED FUNDS.

THE SOURCE OF THIS FUND IS AS FOLLOWS; DURING THE LAST MILITARY REGIME HERE IN NIGERIA, THE GOVERNMENT OFFICIALS SET UP COMPANIES AND AWARDED THEMSELVES CONTRACTS WHICH WERE GROSSLY OVER-INVOICED IN VARIOUS MINISTRIES. THE PRESENT CIVILIAN GOVERNMENT SET UP A CONTRACT REVIEW PANEL AND WE HAVE IDENTIFIED A LOT OF INFLATED CONTRACT FUNDS WHICH ARE PRESENTLY FLOATING IN THE CENTRAL BANK OF NIGERIA READY FOR

PAYMENT.

HOWEVER, BY VIRTUE OF OUR POSITION AS CIVIL SERVANTS AND MEMBERS OF THIS PANEL, WE CANNOT ACQUIRE THIS MONEY IN OUR NAMES. I HAVE THEREFORE, BEEN DELEGATED AS A MATTER OF TRUST BY MY COLLEAGUES OF THE PANEL TO LOOK FOR AN OVERSEAS PARTNER INTO WHOSE ACCOUNT WE WOULD TRANSFER THE SUM OF US$21,320,000.00(TWENTY ONE MILLION, THREE HUNDRED AND TWENTY THOUSAND U.S DOLLARS). HENCE WE ARE WRITING YOU THIS LETTER. WE HAVE AGREED TO SHARE THE MONEY THUS; 1. 20% FOR THE ACCOUNT OWNER. 2. 70% FOR US (THE OFFICIALS) 3. 10% TO BE USED IN SETTLING TAXATION AND ALL LOCAL AND FOREIGN EXPENSES. IT IS FROM THE 70% THAT WE WISH TO COMMENCE THE IMPORTATION BUSINESS.

PLEASE,NOTE THAT THIS TRANSACTION IS 100% SAFE AND WE HOPE TO COMMENCE THE TRANSFER LATEST SEVEN (7) BANKING DAYS FROM THE DATE OF THE RECEIPT OF THE FOLLOWING INFORMATIOM BY TEL/FAX; 234-1-7740449, YOUR COMPANY'S SIGNED, AND STAMPED LETTERHEAD PAPER THE ABOVE INFORMATION WILL ENABLE US WRITE LETTERS OF CLAIM AND JOB DESCRIPTION RESPECTIVELY. THIS WAY WE WILL USE YOUR COMPANY'S NAME TO APPLY FOR PAYMENT AND RE-AWARD THE CONTRACT IN YOUR COMPANY'S NAME.

WE ARE LOOKING FORWARD TO DOING THIS BUSINESS WITH YOU AND SOLICIT YOUR CONFIDENTIALITY IN THIS TRANSATION. PLEASE ACKNOWLEDGE THE RECEIPT OF THIS LETTER USING THE ABOVE TEL/FAX NUMBERS. I WILL SEND YOU DETAILED INFORMATION OF THIS PENDING PROJECT WHEN I HAVE HEARD FROM YOU.

YOURS FAITHFULLY,

DR CLEMENT OKON

NOTE; PLEASE QUOTE THIS REFERENCE NUMBER (VE/S/09/99) IN ALL YOUR RESPONSES. [5]

The scam sounded so convincing that it worked for many years. The selling point of this scam was the typical get rich quick deal. The official look and feel of the email, also helped sell this scam, to those who would otherwise throw it away as spam. The thing that sets the “Nigerian 4-1-9 scam” apart from most phishing attacks, and what most likely made it so successful is the victims received correspondence from the originators of the scam. This correspondence would continue till the scammers got what they were looking for. What they were looking for in all cases was the victim to send their bank

[5] www.secretservice.gov/ofect419.shtml

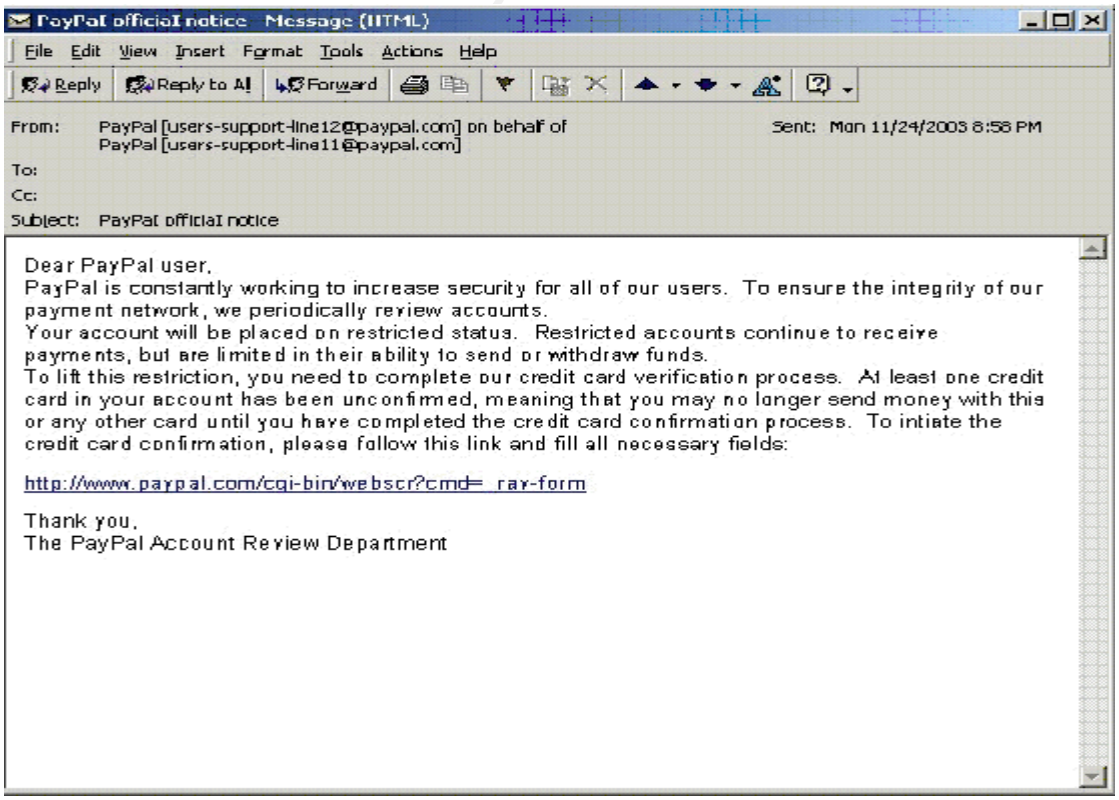
account information. In some cases, letters were sent on official looking letterhead. There was one death linked to this scam, when an American traveled to Nigeria, in an attempt to receive his money, and was attacked by local thugs. The emails for this scam date back as far as 1995, to as recent as 2003.

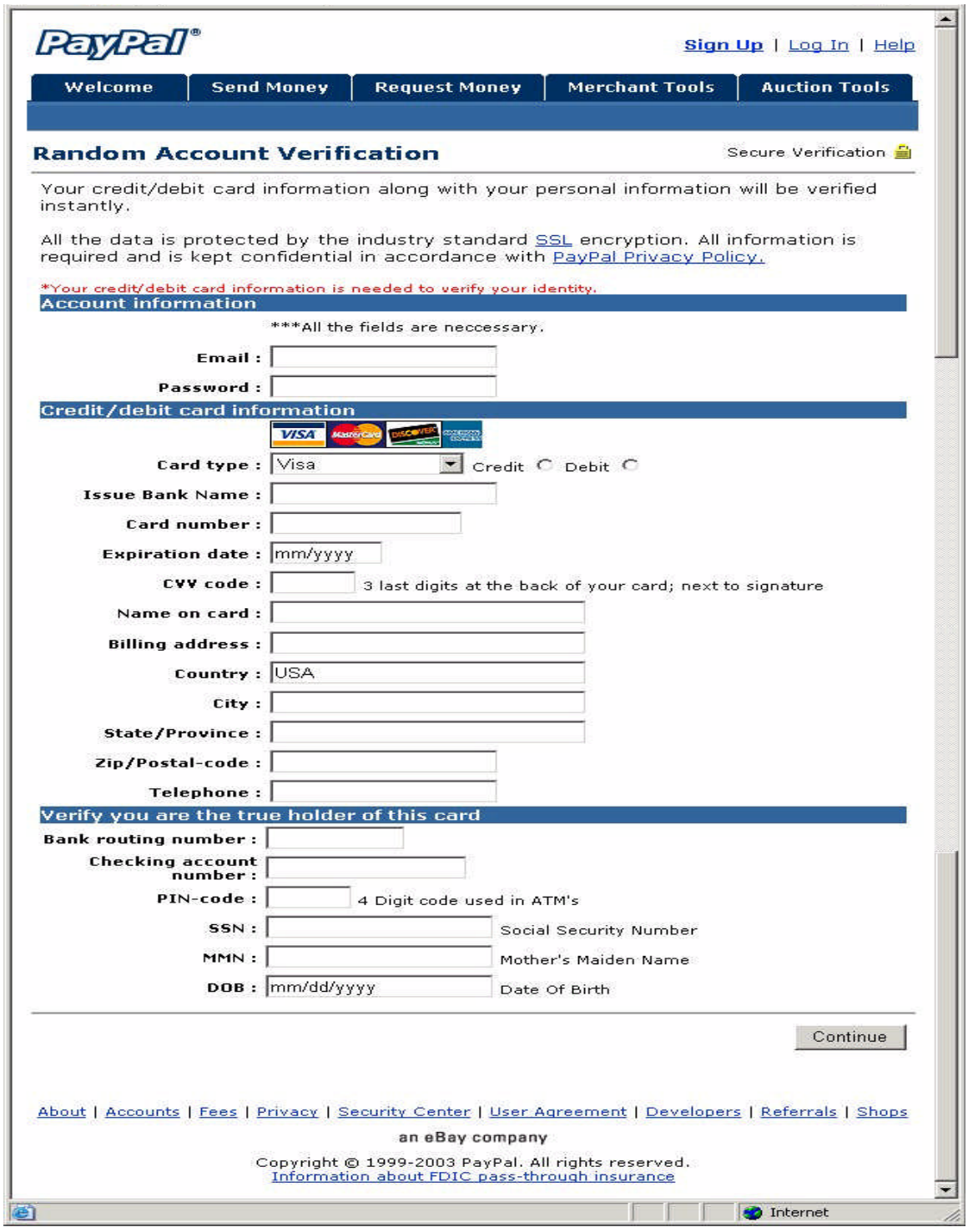
Email with link to phishing website

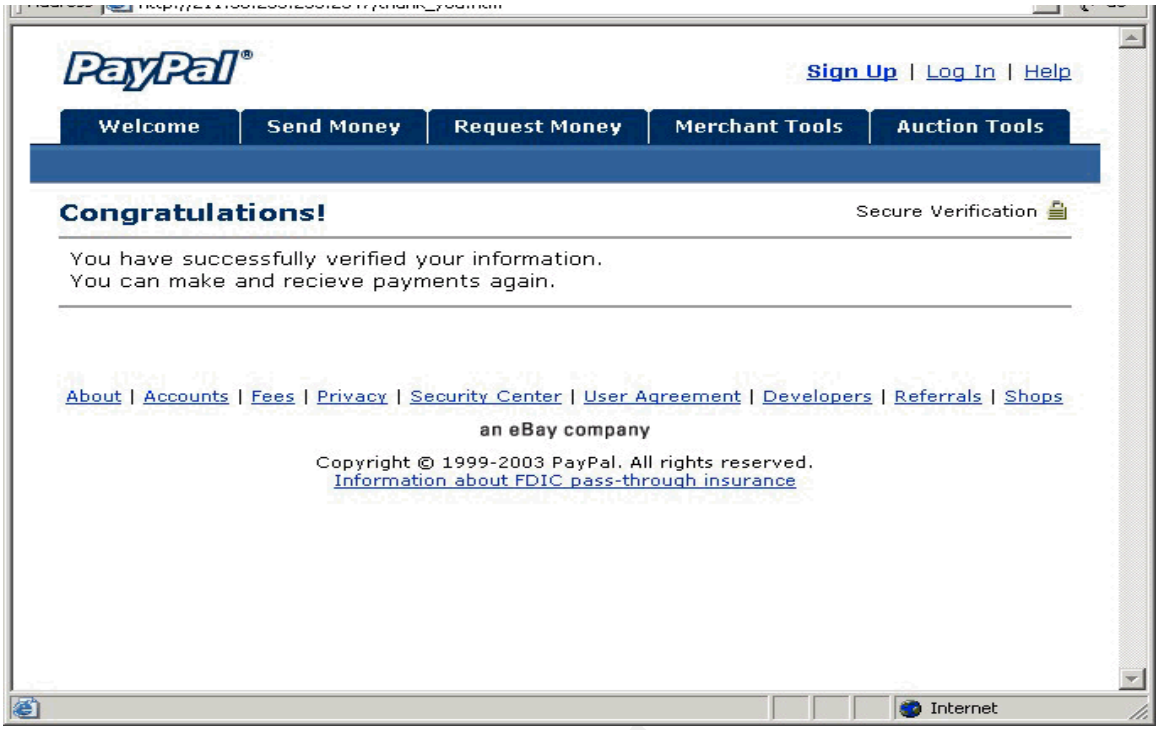
This phishing scam conveys a sense of urgency in its message. The respondent believes that they must respond quickly in order to avoid unwanted consequences.

This scam actually hits home for me. My wife received an email asking her to update her Pay Pal account information. Although unusual, the request made some sense, since she hadn't used her Pay Pal account for some time now. She clicked the attached link and was taken to the Pay Pal login page. After logging in with her username and password, she received a successful login message. She was then redirected back to the Pay Pal login screen. It was at this point she became a bit suspicious, so she closed the window. The scam was successful. The link within the email directed her to a fake Pay Pal login page. After harvesting her personal information, she had been directed to the real Pay Pal login page.

The email she received worked similar to this example:




PayPal
Sign Up | Log In | Help
Welcome
Send Money
Request Money
Merchant Tools
Auction Tools
Random Account Verification
Secure Verification
Your credit/debit card information along with your personal information will be verified instantly.
All the data is protected by the industry standard SSL encryption. All information is required and is kept confidential in accordance with PayPal Privacy Policy.
*Your credit/debit card information is needed to verify your identity.
Account information
***All the fields are neccessary.
Email :
Password :
Credit/debit card information
Card type : Visa Credit Debit
Issue Bank Name :
Card number :
Expiration date : mm/yyyy
CVV code : 3 last digits at the back of your card; next to signature
Name on card :
Billing address :
Country : USA
City :
State/Province :
Zip/Postal-code :
Telephone :
Verify you are the true holder of this card
Bank routing number :
Checking account number :
PIN-code : 4 Digit code used in ATM's
SSN : Social Security Number
MMN : Mother's Maiden Name
DOB : mm/dd/yyyy Date Of Birth
Continue
About | Accounts | Fees | Privacy | Security Center | User Agreement | Developers | Referrals | Shops
an eBay company
Copyright © 1999-2003 PayPal. All rights reserved.
Information about FDIC pass-through insurance
Internet



6

The result of our run-in with a phishing scam, was the purchase of a Tag Heuer watch, on EBay for $1100, and sent to an address in the Philippines.

Email with link to compromised legitimate website

The latest and most technically advanced form of phishing. An email is sent with a link to a legitimate website that has been compromised. The compromise will either be at the website itself or at the servers hosting legitimate websites.

An email is sent with a link to a well known web site (ex. Amazon.com, EBay .com, etc.). The scam involves, "using JavaScript to display the genuine site page within another domain using a frame set. By framing the genuine page in one main window of another site's page, the visitor sees the genuine page."[7] This will only work as long as active scripting is enabled. "Users visit certain popular web sites-- including an online auction site, a search engine, and a comparison shopping site—they unwittingly download a piece of malicious java script code attached to an image or graphics file on the site. Without the user's knowledge, the code connects their PC to one or two IP addresses in N. America and Russia. From those systems they unknowingly download a piece of malicious code that appears to install a keystroke reader and probably some other malicious code on the computer."[8] These types of attacks are almost unavoidable. The only real ways to avoid this type of attack is to disable active scripting on internet connections, and to keep virus

[6] http://www.millersmiles.co.uk/identitytheft/oah-3.htm
[7] http://www.millersmiles.co.uk/identitytheft/cssb.html
[8] http://yahoo.pcworld.com/yahoo/article/0,aid,116689,00.asp

protection software up to date.

Solution Selection

It's often stated that companies never as for personal information in emails. This may or may not be true, but this doesn't keep companies from sending other spam- like types of email to customers. The proposed purpose of many if these emails is to keep customers informed and up to date. But, the result is customers become conditioned to no longer read company correspondence as closely. This opens customers to phishing attempts with "Important" and "Urgent" in the subject line. Companies that want to keep themselves and their customer safe must sacrifice this constant updating, and either develops a monthly or weekly summary for customers to stay informed. All corporate communications with customers should follow a standard format in regards to wording and design. Customers should be urged to type in the company URL and follow links rather than receive emails with embedded links. It should be simple and obvious where customers can learn about the latest phishing scams and how to report, if the believe they've been a victim.

Phishing sites are hard to stop, because they don't have to be around very long to gather the information they need. Some sites may be around for a day or even just a few hours. Even if the scammers are found, what happens if they live outside of the U.S., in an Asian or a European country? The bad guys will always ahead of the posse.

Many companies have come up with enterprise level solutions to combat the rise in phishing attacks. Ecommerce sites must be proactive in their monitoring of cross-linked websites, similar named and look a like sites, and possible phishing attacks. The first thing, cheapest thing, and the easiest thing a company can do in the fight against phishing, join the Anti-Phishing Working Group. Basic membership in the group is free. The fees that are collected are used for the continuation and improvement of the group. It is a great resource for information regarding new and old phishing attacks, as well as possible countermeasures. They have some of the industry's leaders in security as members

To solve the issue of sender authentication, solutions such as SPF (Sender Policy Framework), Microsoft Caller- ID, and Domain Keys, graphical sender authentication and S/MIME are possibilities.

Sender Policy Framework

An email is sent to a recipient, the recipient's email gateway server, does a DNS query of the sender, to get a list of approved sender IP addresses. If the email originates from an IP address on the approved list, the email is passed onto the recipient. If the IP address does not appear on the approved IP address list, the email is dropped.

Microsoft Caller- ID

An email is sent to a recipient, the recipient's email gateway server does

a DNS query of the sender. The Email gateway server contains a XML list of approved IP addresses. The sender IP addresses is compared to the list. If the email originates from an IP address on the approved list, the email is passed onto the recipient. If the IP address does not appear on the approved IP address list, the email is dropped.

Domain Keys

An email is sent to a recipient with a digital signature in the header. The recipient's email gateway server does a DNS query of the sender and returns a public key. The sender's digital signature is compared to the generated public key. If the signature matches email originating from an IP address of the approved list, the email is passed onto the recipient. If the IP address does not appear on the approved IP address list, the email is dropped. This solution has been adopted by Yahoo.

Graphical Sender Authentication

PassMark Security (www.passmarksecurity.com) allows companies to embed a personalized image in outgoing emails and on their webpage. An email is sent to a recipient, the recipient's email gateway server, does a DNS query of the sender, to get a list of approved sender IP addresses. The list of approved IP addresses link to a software program running on the server. The server then associates the IP address with a graphic, which is then sent to the recipient. The graphic allows the recipient to authenticate the sender of an email. Customers are taught to only open emails or access web pages, if they see their personalized image.

S/MIME (Secure Multipurpose Internet Mail Extension)

An email is sent to a recipient from a sender, who has been authenticated through a certificate granted by a third party certifying Authority (i.e. VeriSign, GlobalSign, etc.). An S/MIME digital signature is created using the certificate and applied to the email. The recipient's email server, using S/MIME authenticates the digital signature, and the email is passed onto the recipient. If the IP address does not appear on the approved IP address list or have a digital signature, it is dropped. Email services such as Yahoo and Hotmail, do not support S/MIME at this time.

Some smaller scale and software based solutions have also been proposed. Digital Envoy, maker of IP Inspector E-scam allows companies to set up a "Phishing account". With this account in place, a company can instruct customers to send all suspicious emails to the "Phishing account" This account links to Digital Envoy's IP Inspector E-scam product and the company itself, where it is scanned for validity, the source IP is verified, and any embedded URL's are checked.. If it is found to be a phishing email, the company can give early warning to its customer base, as well as an example of the scam. Companies such as, Netcraft (http://news.netcraft.com), based in the UK and Cyveillance (www.cyveillance.com), will continually scan the web for possible

misuses of participating companies' web sites. They also scan DNS servers for possible similarities. Microsoft has even brought up the possibility of charging companies for verification, if they want to send emails to their hotmail and MSN customers. "With some 170 million claimed regular users of Microsoft email"[9], companies may feel compelled to pay the varied fee based on the amount of email they plan to send for fear of possibly being rejected by the ISP's email servers.

Spam blocking software, email filtering software and Anti- Virus software, can help with the phishing problem on a corporate level. Anti-Spam solutions such as Barracuda's Spam Firewall or Brightmail's Anti-Spam, allow for email filtering, as well as attachment scanning. This will cut down on the number of unwanted or suspicious emails allowed to customers. Products such as, McAfee Virus Scan and Norton's Anti Virus will scan emails as they pass through the email server, as well as protect on the desktop level. Both can be set to update their virus signatures automatically. A firewall, whether hardware or software based, should be in place. This will allow for the blockage of unwanted traffic in or out of the network. Some of the newer phishing attacks, have used ports usually reserved for internal traffic to propagate their scam externally.

But corporate solutions only work in the corporate world. What happens when people are at home using their own PC's? Home users account for the majority of phishing attacks. Maybe it's because people are more at ease and trusting at home, or maybe they are just naïve. Either way, another solution must be explored to help halt the rise in phishing attacks, which will support both the corporate and the home user. That solution is user education.

User education should start the minute a new computer is purchased. It should start the first time and every time the internet is accessed. Phishing scams prey on the ignorance of the recipient. The only solution to ignorance is education. If you want someone to really learn something, you don't just introduce it to them once, you teach them, test them, and then teach them again.

How many viruses or worms have been brought into network systems, by users who weren't sure who the email they received was from, but opened it anyways? What would cause someone to think that it's okay, to fill out a form in an email with personal information, for an online account they haven't used in over a year? User education is at the heart of the phishing issue. Companies that want to continue doing online business must take user education very seriously. It must be made clear to all users, at work and at home, that phishing scams are a real problem and all the technology in the world is useless, if the user doesn't take the time to think. As stated earlier, it must be very clear to customers, where and how to report and stay informed of phishing scams. How hard would it be for an online business to send its customers correspondence by normal mail, when it wants to update personal information? This way, if they receive a phishing email, they know for sure that the email is a scam. Communication and education are the easiest ways for a company to help its

[9] Http: //www.pcpro.co.uk/news/news_story.php.?id=57163

customers, as well as itself, through this recent flurry of phishing attacks and into the future. Companies need to understand what is really at stake: Customer confidence and the future of ecommerce

In summary, a new email scam is sweeping the internet called phishing. It cuts at the very core of ecommerce. Businesses are losing revenue, because they have to reverse charges their customers did not make. People are having their personal information stolen, when they believe they are just doing normal business with their favorite sites. IT security companies are hard at work trying to find a solution. Right now, the best way to deal with phishing is a multi-tiered business solution, which includes: firewalls, anti- virus software, anti-spam software, web monitoring, and some form of sender authentication. But even with all these in place, the bottom line is educating the users. For without educated users, all these security implementations are useless.

References:

1. Berlind, David. “Phishing: Spam that can’t be ignored”. Tech Update. (7 Jan. 2004). URL: http://techupdate.zdnet.com/techupdate/stories.main/Phishing_Spam_that_can’t_be_ignored.htm (9 Jul. 2004).

2. Bright, Matt. “Spoof Email Phishing Scams and Fake Web Pages or Sites”. (23 Feb. 2004). URL: http://www.millersmiles.co.uk/identitytheft/gonephishing.htm (22 Jun. 2004).

3. Federal Trade Commission. “How not to get hooked by a ‘Phishing’ Scam”. URL: http:// www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm (June 2004).

4. Gaur, Nalneesh. “Hooked”. Information Security. July 2004 (2004): 58- 61.

5. Greek, Dinah. “Phishing rocks the e-commerce boat”. Vnunet.com (24 May. 2004). URL: http://www.vnunet.com/news/1153549 (22 Jun. 2004)

6. Hines, Matt. “Gartner: Phishing on the Rise”. Cnetnews.com. (15 Jun. 2004). URL: http://zdnet.com.com/2102-1105_5234155.html?tag=printthis. (17 Jun. 2004).

7. Jack, Rodney. “Online phishing uses new bait”. Vnunet.com (6 Apr. 2004). URL: http://www.vnunet.com/news/1154101 (22 Jun. 2004)

8. Jaques, Robert. “Gartner warns banks of spyware fraud”. Vnunet.com (16 Jun. 2004). URL: http://www.vnunet.com/news/115924 (22 Jun. 2004).

9. Loftesness, Scott. Responding to “Phishing” Attacks, Glenbrook Partners. .URL: http://www.glenbrook.com/opinions/phishing.htm (3 Sept. 2004).

10. Malone, Steve. “Email marketers told: Pay upfront if you want to send email to MSN or Hotmail”. Computer Shopper. (5 May 2004). URL: http://www.pcpro.co.uk/news_story.php?id=57163 (9 Sept. 2004).

11. Millard, Elizabeth. “Gartner: Phishing on the Rise”. www.EcommerceTimes.com. (6 May 2004). URL: http://www.technewsworld.com/story/33683.html (3 Sept. 2004).

12. Niccolai, James. Paul Roberts. Martyn Williams “Hackers Attack Through Popular Web Sites”. IDG News Services. (25 Jun 2004). URL: http://yahoo.pcworld.com/yahoo/article/0,aid,116689,00.asp. (25 Jun. 2004).

13. Pruitt, Scarlet. “Web Attacks Targets Financial Data”. IDG News Services. (25 Jun 2004). URL: http://news.yahoo.com/news?tmpl=story&cid=1093&u=/pcworld/20040625/tc_pcworld/. (25 Jun. 2004).

14. Radcliff, Deborah. “Phear of phishing”. NetworkWorldFusion (31 May 2004). URL: http://www.nwfusion.com/cgi-bin/mailto/x.cgi (3 Sept. 2004).

15. Radmussen, Rod. “Phishing Prevention: Making yourself a hard target”. Version 1.0. Internet Identity. April 2004.

16. Ranger, Steve. “US falls hook, line & sinker for phishing”. Vnunet.com (06 May. 2004). URL: http://www.vnunet.com/news/1154975 (22 Jun. 2004).

17. Savage, Marcia. “This threat could kill e-commerce”. SCMagazine. May 2004. (2004): 22- 25.

18. Tally, Gregg. Roshan Thomas. Tom Van Vleck. “Anti-phishing: Best practices for institutions and consumers” McAfee Research. (March 2004). URL: http://www.mcafeesecurity.com

19. Thomson, Iain. “Phishing still on the increase”. Vnunet.com (17 Mar. 2004). URL: http://www.vnunet.com/news/1153549 (22 Jun. 2004)

20. Thomson, Iain. “Phishing using smarter hooks”. Vnunet.com (20 Apr. 2004). URL: http://www.vnunet.com/news/1154522 (22 Jun. 2004)

21. Tumbleweed Communications Corporation. Using Digital Signatures to Secure Email and Stop Phishing Attacks. (2004). URL: http://www.tumbleweed.com.

22. United States Secret Service. Public Awareness Advisory regarding”4-1-9” or “Advance Fee Fraud” Schemes. (2002). URL: http://www.secretservice.gov/alert419.shtml (2 Aug. 2004).

23. URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci916037,00.html. (17 Jun. 2004).

24. URL: http://www.antiphishing.org/news/03-31-04_Alert-FakeAddressBar.html (31 Mar 2004).

25. URL: http://www.antiphishing.org/phishing_archive.htm (April 2004).

26. URL: http://www.digitalenvoy.net/solutions/ipi/escam.shtml (3 Sept. 2004).

27. URL: https://www.paypal.com/cgi-bin/webscr?cmd=p/gen/fraud-prevention-outside

28. Whipp, Matt. "Anti-Phishing technologies have no effect on spam". Computer Shopper. (7 Sept. 2004). URL: http://www.pcpro.co.uk/news_story.php?pid=20040907103346 (9 Sept. 2004).