The Layman’s Guide To Phishing and Pharming

Joshua J Sawyer

East Carolina University
Abstract

In presenting the concepts of phishing and pharming, this paper gives the reader a descriptive, yet active view. The terms themselves are described, as well as possible avenues of action that can be used to prevent and resolve these types of computer crimes via real-life examples from the field. The primary target of this paper is the personal/home user. However, the analysis given will certainly apply in a business setting as well, although the solutions described may need to be adjusted to compensate for the higher frequency of potentially fraudulent communications received. The concepts discussed here should be considered mandatory knowledge for those who seek to safeguard their personal information or that of their employers.
The Layman’s Guide To Phishing and Pharming

Most individuals in computer related fields are no doubt familiar with hearing the terms “phishing” and “pharming”, but confusion abounds as to what each actually refers to and how to deal with them. This paper addresses both of these terms, but most exclusively, the former.

Let’s begin with phishing. In reality, phishing is somewhat related to a fish, in that it is used to ‘fish’ for information. Specifically, phishing is a term used to describe phony email messages, often purportedly from financial institutions, that ask for personal information such as account or Social Security numbers (David Bank, 2005, ¶6). These fraudulent emails are often very convincing and look identical to the genuine ones from the company they are imitating. This type of attack relies on the concept of social engineering, which is the method of abusing a person’s concept of trust. The hope is, if you can convince someone by any means that they should comply with your wishes, they’ll give you information you need to compromise systems and would have a minimal chance of getting otherwise.

In general, one of the main reasons attributed to the failure of computer security is either the wrong setup, or mis-understanding of a system by the user (Jendricke, Gerd tom Markotten, 2000, ¶2).

A recent example of social engineering is ChoicePoint, a broker of personal information, which was targeted by scam artists (Schwartz, 2005, ¶2). Using about 50 fake businesses as fronts, the scammers opened authorized ChoicePoint accounts and purchased about 145,000 reports on consumers in Choicepoint’s databases (Schwartz, 2005, ¶2). This illustrates one of many important points: Security is only as good as its weakest link. Regardless of the encryption or other safety measures deployed to protect the systems and information, the home user / employee can override this by giving information to criminals, thus bypassing the entire security
mechanism altogether. In this case, Choicepoint believed these were legitimate businesses by the way the scammers had built up their websites and identities.

Contrary to popular belief, the typical phisher isn't a movie-style villain, but rather an overseas teenager; one who belongs to a social and economic infrastructure that is both remarkably sophisticated and utterly ragtag (Gomes, 2005, p. B1). These criminals work around the clock formulating ways to get users to divulge personal information via email and fraudulent web sites. The types of online fraud that authorities are seeing are of various types, such as fake investment and business opportunities, fraudulent online auction sites, fake credit card issuing, and many others (Rusch, 1999, ¶3). A newer, more specialized form of phishing, called “Spear Phishing”, occurs when attackers create email messages that are designed to look like they came from the recipient's company or organization, such as information-technology or human-resources departments (Bank, 2005, ¶7). The following section is designed to assist you in identifying and dealing with these phishing attempts.

The first step in dealing with a phishing attempt is to identify it. Contrary to the belief of many users, email is not sent directly from the sender to the recipient. It travels through many systems while in transit. A typical email passes through at least four computers before reaching its destination (Lucke, 1997-2004, ¶5). As it passes through these computers, logs called headers are added to the email, similar to a postmark, that can give the recipient a clue to the origin of the email itself. Occasionally, especially in spam messages, some of the information in these headers may be forged, but there is usually enough evidence to trace the email back to its origin, and report it to the appropriate administrator(s). This is one of the areas we will focus on.

I have received, logged and reported hundreds of phishing scams from my personal email over the course of about a year. I am glad to report that for over 90% of them, I receive emails
back from the appropriate administrators informing me that they have taken the necessary
actions against the user accounts I reported. My goal is to use illustrations from my experiences
to guide you in this technique. Once informed, you can also begin to fight back against the
problem of spam, rather than simply deleting it and leaving the spammers up and running to send
further phishing attacks.

To illustrate the makeup of these spam emails, shown is an actual phishing email I
received in my mailbox at: josh500@cluemail.com (Figure 1). Note the enticing but drastic
message in the body of the email, promising the reader may be the recipient of “gold and
diamonds” if they do as the scammer asks. This is quite drastic and easier to catch than most
fraudulent emails, but keeps the user inquisitive enough, the fraudster hopes, to reply. Also note
that the sender wants the recipient to keep this transaction ‘confidential’ to prevent them from
sharing the email with others, becoming suspicious, and potentially discovering the criminal
intent behind the email. The first step in dealing with phishing solicitations is identifying them.
How can the recipient be sure they aren’t missing out on a legitimate opportunity? First, one
should take a moment to see if they remember having any dealings with the organization /
company in the past. If so, then they should go to the company’s website directly and check to
make sure the email’s content matches the email just received. If one cannot recall having
any dealings with the company in question, or in this case, has never heard of it because it is a
quite drastic and obvious email from a fraudster requesting your information, then it is most
likely a fraud, especially when asking for contact information, financial assistance, or any other
type of sensitive information. Never reply to email messages that ask for personal info (Baker,
2005, ¶5). Doing so alerts the fraudster that he/she has sent the email to a valid address, and you
will receive more emails in the future.
The specific phishing example shown (Figure 1) is called a ‘419’ or ‘Nigerian scam’, with the 419 being derived from an article of the Nigerian penal code under which it is prosecuted (Wein, 2005, ¶1). These types of scams, as in this example, often rely on users to be in a hurry to collect promised funds or valuables. The scammers hope that the recipient of the email will act before thinking. They will do just about anything imaginable to pry personal information from a potential victim (Childers, 2005, ¶2).

So, what to do with this fraudulent email? Once it is determined that it is not legitimate, the source needs to be identified so the necessary administrators can be notified. To do this, one must view the email headers. Never rely on the text in the body of the email, because it is most likely fake, as certain parts of the headers frequently are as well.

Let’s now step through all the email headers to see what information we can glean about the source. Headers are normally read starting at the bottom with the originating headers, and working up to the top where the headers most recently added are. This may vary however, and for the sake of simplicity, we will simply go from the top to the bottom. Note in the top of the email (Figure 1) the value: ‘Return-Path: p_1263@walla.com’. This is the address to which bounced mail will be sent, and should match that of the ‘From:’ value, which it does. The next value, ‘Received:’ is perhaps the most useful value (Univ. of Bath, 2004, ¶10) in the headers, as it identifies the machine(s) through which the email was transferred. The server name in a header of the format ‘Received: from [server name] (server name[10.202.2.203])’ can be easily forged and cannot be trusted. However, a more reliable fingerprint is the ip address shown beside the servername, i.e. ‘10.202.2.203’ in this example. This is later discussed in further detail. The second value (Figure 1):

‘Received: from mx4.internal (mx4.internal [10.202.2.203]) by server3.messagingengine.com
(Cyrus v2.3-alpha) with LMTPA; Sat, 10 Sep 2005 00:14:00 –0400’ refers to the mail server for my email provider, so this does not yield any information about the sender and is ok. This is the last header that was added to the email before I read it, so it is, not surprisingly, the mailserver for my email provider. The next line: ‘X-Sieve: CMU Sieve 2.3’ simply refers to an XML transformation language used by my email provider, so this is also ok. A small note about X-headers is that they are user – defined and used by mail programs and applications. This means that they are primarily used to transfer information to an email program. They are useful for confirming information found in the other header values, but should not be relied upon alone, as they are easily faked. The next value: ‘X-Delivered-to: josh500@cluemail.com’ obviously specifies the target (recipient) of the email. This is my address, and is correct. The next line: ‘X-Mail-from: p_1263@walla.com’ presents some solid information about the sender’s email address. This reflects that this email was sent via an address at walla.com. This can, however, be forged, so we will make a note of this and confirm / deny it’s value later on. The next value: ‘Received: from omail11.walla.co.il (omail11.walla.co.il [192.118.71.131] by mx4.messagingengine.com (Postfix) with ESMTP id 8CA94AE809A for <josh500@cluemail.com>; Sat, 10 Sep 2005 00:13:59 -0400 (EDT)’ reveals a treasure trove of information! Here we see that the email was received by my mail provider’s mailserver ‘(mx4.messagingengine.com) from omail11.walla.co.il’. How can we check to make sure the email’s source is actually ‘omail11.walla.co.il’? We can run a reverse DNS lookup on the ip address 192.118.71.131 and see who it is registered to. If the from server (omail11.walla.co.il) is spoofed, or fake, then the ip address will reveal another (the true) provider. By submitting a query on the ip address here: [http://www.dnsstuff.com](http://www.dnsstuff.com), we are able to see that the result comes back to:
‘192.118.71.131 PTR record: omail11.walla.co.il’. This tells us that the email was indeed sent through the walla email system.

Let’s go a little further to find out more. The next value:

‘Date: Sat, 10 Sep 2005 07:13:28 +0300’, tells us the email was received by the walla mailserver at that date and time. The next line: ‘Received: from ([80.87.82.125]) by omail11.walla.co.il ([192.118.71.131]) with HTTP; Sat, 10 Sep 2005 07:13:27 +0300’, shows that the walla mailserver received the email from its author at ip address 80.87.82.125. Is the pattern starting to make sense? This is precisely why some fraudsters add more fake headers and try to modify all they can on the legitimate ones to try to confuse the reader and make it more difficult to identify the sender. If the lines are examined carefully, even if some are forged, one can retrieve useful info from the email headers. This ip address (192.118.71.131) matches that of the other header, so we have further evidence that the email was transferred through the walla email system. The ‘from’ ip address, 80.87.82.125, was the fraudster’s computer ip address at the time the email was sent from the fraudster to the walla network. This ip address can be spoofed, by using a proxy server or anonymity service, but usually this is not the case. It can most likely be traced to a provider, but may be used by an isp or other company which uses a pool of ip addresses, making it difficult to narrow down to a specific user. Even if this is the case, this provider will have logs which may help if the email’s contents were of a serious nature.

Continuing on, the next line: ‘From: =?UTF-8?Q?=50=72=69=6E=63=65=20=43=68=75=6E=6B=79=20=54=61=79=6C=6F=72?= p_1263@walla.com’, looks interesting, as if it is some type of a code. It actually is. It has been encoded on purpose to avoid possible detection by spam filtering techniques. A novel idea? The fraudster actually hex encoded the text containing the description of the ‘From’ field.
This will appear to the left of the email address: ‘p_1263@walla.com’ in the body of the email when the recipient reads it. To decode the text, I used a shareware program called ‘EType Mail Decoder’ by Alexander Gorlach, available at: http://www.gorlach.etype.net/ecoder. The resulting decrypted text (Figure 2) reveals the sender’s ‘From’ identity. This is also obviously forged, but the sender has attempted to circumvent any spam filtering technologies by encoding it. This is a common practice with some phishing attempts.

The next line (Figure 1): ‘X-Sender: p_1263@walla.com’, shows the sender’s email address. This can be forged also, so we will tuck this away for later verification. The next two lines (Figure 1): ‘X-Originating-Email: [p_1263@walla.com]’ and ‘X-Originating-IP: [80.87.82.125]’ are redundant in that they are the same as we previously discovered. This is a sign that we’re on the right trail. Our next value (Figure 1): ‘Subject: =?UTF-8?Q?=70=6C=65=61=73=65=20=61=73=73=69=73=74=20=6D=65=2E?=’ shows the sender encoded the subject of the email as well. The subject would almost certainly be scanned by spam filtering technology, so he/she wanted to be sure to encode this to avoid possible detection. The decrypted text (Figure 2) shows the subject the sender gave the email. This is a curious subject to be sure. No explanation or identification, just ‘needing assistance’.

The next line in the email headers (Figure 1): ‘Message-Id: 1126325607.953000-26010223-25025@walla.com’ is significant in that it is a somewhat unique identifier attached to our specific email message. This should match that of the sending email provider, and if not, then it is forged. This does match, so we have a further confirmation of the path the email took. The next statement (Figure 1): ‘MIME-Version: 1.0’ simply stands for Multipurpose Internet Mail Extensions, and is an internet standard that states how messages must be formatted so that they can be transferred between different email systems (Univ. of Bath,
The next value we see (Figure 1): ‘Content-Type: multipart/mixed; boundary="------=_EREZ_P_WallaMail_93488_9288_P_0”’, specifies the type of content that will be used. This is related to the content type of the email body, so it isn’t useful for our tracking purposes. The last line of the headers (Figure 1): ‘To: undisclosed-recipients’, shows that the sender used a mailing list of email addresses to send the email out to. This means that we are most likely not the only recipients of this particular email.

Based on the information given, we have substantial evidence that the email originated from a user who sent it via walla mail servers. What can we do about this?

The second step in dealing with phishing emails is to report them, once identified. We have already identified the source with two ‘Received:’ headers (Figure 1) that have matching ip addresses. We need to alert an administrator at the walla email provider that they have a Nigerian scam being sent by a user from one of their email accounts. This brings up another important point. Most fraudsters use ‘free’ email account providers, as they can set many of them up quickly. Once one of their accounts is suspended, they set up another one. This is where their internet provider can step in. They can monitor the ip addresses of the fraudster’s computer when they try to login to or set up additional accounts to use for phishing. Over time, they may be able to locate and catch the offending user if it gets bad enough. For this to happen however, the phishers must be reported, so the provider knows what’s going on. To do this, I use a website that lists most of the free email providers that phishers use, such as yahoo.com, hotmail.com, and many others. The site also shows further information on Nigerian fraud schemes and how to report fraudulent emails: [http://www.joewein.de/sw/419-freemail-abuse.htm](http://www.joewein.de/sw/419-freemail-abuse.htm). It’s a good idea to print this entire web page out for future use. We have determined that the email was sent from the walla email provider, so the next step is to find the walla’s abuse email address to send the
message to. Before we do this, we need to open the original email message, show full headers, then choose to forward the email. Different mail programs will have different ways to show the full headers. If in doubt on how to show them, consult the help in your email program. Once we have the full headers displayed, we are sure to forward them, along with the original email body, to the appropriate administrators. In this case, we will report them to walla, so we go down the list of providers here: http://www.joewein.de/sw/419-freemail-abuse.htm and search for ‘walla’. If your email provider’s name is not listed here, then go to google and search for “abuse domain.com”, with ‘domain.com’ being the provider your fraudulent email was sent from. You may need to read the company’s terms and conditions page to find their abuse email address. I have had to do this for some email providers in Argentina, Poland, and many others. The walla abuse email contact from the joewein website is ‘abuse@walla.net.il’, so we send a copy of the full email, including headers, to this email address, and tell them we received the included email, and that it was sent from their email system. We ask them to please do what they can to stop their users from sending these types of fraudulent emails, and thank them for their time. The reply I received shortly afterwards (Figure 3) shows that this email provider was clearly appreciative to have been informed of the illegal activity so they could resolve it. This is truly the ultimate in fighting spam and phishing emails.

Instead of ignoring the problem by deleting them while others can still fall victim to them, simply taking the time to report them ensures that everyone will have less of them to deal with. It only takes one person to report the sender, and many people can be spared from potentially replying with sensitive information. Assuming that we reported the email, even if a user who is too trusting actually believed the content of the fraudulent email and replied to it, if the provider closed the account, all the user would have lost is the time they took filling the form out,
The Layman’s Guide

Instead of becoming another victim. They will receive a ‘user unknown’ or ‘mailer deamon’ error email instead of an email perhaps requesting even more information. In this way, just one person can make a huge difference in fighting the war on online scams.

There is software available for corporate and business use, as it would not be timely to do this to every email message received, but it will certainly help those who receive only occasional emails and want to help fight fraud. How did they get your email address to begin with? This is an excellent question, and phishers use various ways to get email addresses. One way is to obtain them from an email address harvester, a type of software which scans the internet, bulletin boards, posts, web sites, advertisements, etc, for email addresses, then adds the harvested addresses to one large list the phisher can use for sending out fraudulent emails. A second method is to obtain this information from compromised systems or databases. The recent loss of information from well-known companies emphasizes the risk of having this information leaked. A third way is through further social engineering! The phisher may simply call a business or institution with the information he/she has already gathered, and attempt to appear as if he/she is entitled to additional information, such as email addresses, passwords, and other sensitive information, or even something as simple as when a certain person will be leaving the office, so they can call back later and try their scheme again if the first attempt was unsuccessful. A fourth method is by using a random email address generator. This is a program that generates random email addresses, such as: john.smith@cs.com, or bill.w.eure@mail.org. It takes known domains, such as gmail.com, and adds names either from a dictionary file or a random generator to them in an attempt to come up with a valid email address. The fraudster then sends his/her fraudulent email out to all of these addresses, hoping a few are valid and in use by some unsuspecting individuals. This is why it was stated earlier that it’s never a good idea to reply to a phishing
email for any reason, as the phisher has no way of knowing your email is active other than he/she did not receive a ‘user unknown’ or ‘mailer daemon’ error message after the fake email was sent.

An example of a ‘Nigerian 419’ scam (Figure 1) has been shown and ways to combat them have been discussed. However, not all phishing emails take on this same style. Others mimic and appear to be from much more legitimate sources, such as Ebay, Paypal, a trusted online bank, etc, and more fraudulent and misleading techniques are employed. Shown is an example of one of these less obvious and more sophisticated phishing attempts that I received in my inbox (Figure 4). Notice from the body of the email that this fraudster is masquerading to be from Paypal, and tells us that it is in our best interest to act as soon as possible to prevent anything from happening to our Paypal account. This fits in with the typical style of phishing emails. They appear to be extremely time-sensitive and convey the idea that delaying could result in problems. Some of these more recent phishing emails are taking on a much more legitimate look than the standard ‘419’ scams, mimicking companies such as Ebay. The email looks exactly like Ebay’s bid status page, and claims that you have just bid on a $12,000 car. The email provides an all too-convenient button, which says “Cancel Bid”. The hope is that you will carelessly click on the button and submit your login information to cancel the bid, which never existed to begin with, thereby giving the phisher full access to your Ebay account, credit card, and perhaps various other personal information as well.

As compared to our previous email (Figure 1), this fraudulent letter has some differences. First, it is impersonating a business entity, not an individual. Second, it has two paths we need to investigate rather than just one: the email provider from which the email was sent, and the link included in the bottom of the email, which will help us to ‘activate’ our account. What is the purpose of this email? None other than to steal the information we enter into the browser when
we visit the link in the email. We will return to this later. Let’s look at the headers to see what we can gather. The first line of the headers section (Figure 4): ‘Return-Path: albiciousnet@clust07-www01.powweb.com’ suggests that this email will be used for any bounced email messages. It can be easily spoofed, so we won’t rely on this for anything but a suggestion. The next group of lines (Figure 4): ‘Received: from mx1.messagingengine.com (mx1.internal [10.202.2.200]) by server3.messagingengine.com (Cyrus v2.3-alpha) with LMTPA; Sun, 24 Jul 2005 07:54:05 -0400’, is information from my email provider’s servers, so we can ignore this. Skipping down to the next Received header (Figure 4): ‘Received: from clust07-www01.powweb.com (clust-07.www01.powweb.com [66.152.98.71])’ tells us that this email originated from powweb’s mail servers. To check, we again do a reverse DNS lookup on the ip address 66.152.98.71 at http://www.dnsstuff.com, and we receive the following response: ‘66.152.98.71 PTR record: clust07-www01.powweb.com. [TTL 3600s] [A=66.152.98.71]’.

We now have verification of where the email originated from. We can now search for powweb’s abuse email address and send a copy of the email with headers to the appropriate administrator at powweb. We have only solved half of the problem, however, as this phisher has included a link to enter information into. The email is simply being used as nothing more than a lure to impress the user into believing it is genuine, and proceeding to the fraudulent link displayed. Note the stealthy method used to ‘hide’ the real url in the body of the email (Figure 4). It says “Click here to activate your account”. Notice however, that when I moved the mouse pointer over the link (and did not click), the following url was displayed: ‘http://www.yang.org.hk/images/Paypal/error.html’. This definitely is not a genuine Paypal url. The link, when visited, yielded an exact copy of the Paypal login page, except that it was not located on Paypal’s servers. Sometimes the url, instead of saying “Click here to activate your
account”, will appear to be a valid address, such as
“https://www.Paypal.com/login/cgi_scr?+234aXc4r9” or similar. Never rely on what the link appears to be in the body of the email – it is most always fake. To reveal the true url, right click the link, then choose to open it in a new window, or select ‘copy link location’. Pasting this into a word processor will reveal the true url you are being sent to. This url’s domain does not begin with Paypal.com. Instead, it is www.yang.org.hk. We can now do a whois lookup on this domain and see who it is registered to. To do this, we again go to http://www.dnsstuff.com, and enter ‘yang.org.hk’ into the whois query box. The result (Figure 5) shows that the domain is registered to a company in Kowloon, Hong Kong! We could have guessed this simply by noticing the .hk extension on the domain, but we now have further information. Not exactly the company you would like to give your Paypal login information to, ay? Sometimes whois information is also forged, so we may need to visit the link to see if we can ascertain the web hosting company in charge of the website. For now, we can use the email and contact information to notify the administrative contact about the abuse being hosted on his/her domain. Sometimes the website is exclusively used for phishing, but at other times, the company owning the domain has no idea an employee or other individual has added a fraudulent page to their website. In either case, it won’t hurt to notify the contact we found. The next step could be to actually open just the domain of the fraudulent link (http://yang.org.hk) in a new window, in order to find additional abuse and other contact email addresses. The addresses you will be looking for will be in the form of abuse@domain.com, postmaster@domain.com, or similar. Doing this will both alert the company through which the phishing email was sent, and the company owning the domain the fraudulent site is hosted on. This will allow them to take the necessary actions to correct the problem. Only in rare cases have I experienced providers who did not reply to my complaints, or
did not seem to want to correct the problem. You will run into these occasionally, but most of the
time, they will be glad to receive the information and will keep the phishers from pulling off
their illegal plans. Hosting webpages for phishing scams can have legal implications for most
hosting companies if they don’t resolve the problem, or create a bad reputation, which may be
even worse to most companies. Instead of logging into a database full of stolen usernames and
passwords, the phisher will receive an error message stating that their account is terminated,
because their illegal activity was reported. Notice that this email subject was not hex encoded
(Figure 4). Some phishing emails do use encoding, and some do not. This one is relying on you
to believe that it is legitimate by appearing as genuine as possible. Notice also (Figure 4) that
they even include a fake Paypal case id number ‘PP-056-245-481’ to further mimic Paypal’s
format. This particular email didn’t include any images from Paypal. Others do, and usually load
them directly from the legitimate company’s website, effectively stealing their bandwidth and
making the email appear identical to the website of the legitimate company!

A common fallacy is the assumption that all websites that have ‘https’ in the beginning
of the url are safe. This is a very dangerous and false assumption. All that is required to make a
website ‘secure’ is the purchase of an ssl certificate, which can be purchased from many sources,
or obtained free of charge! If you rely on the ‘https’ in front of the url as an indicator that the site
is legitimate, then you will be putting your information at unnecessary risk. For example, a user
relying on ‘https’ as an indicator that a website is legitimate would have no problem connecting
to a fake website, such as https://www.paypai.com, which could be a copy of the real Paypal.com
website. If this site was owned by a malicious user or hacker, you would be securely submitting
your login and password information to a hacker’s website! It is only secure in that no one
other than you and the hacker would know your username, password, and other personal
information, but is that real security? Hardly.

If you can’t use the ‘https’ prefix to determine if a website is legitimate, then what can you use to determine a website’s legitimacy? The ‘https’ (SSL) secured status only guarantees that your computer and the remote computer are talking via an encrypted channel. SSL is simply a protection method used to secure traffic traveling over the internet (Wagner, Schneier, 1996, ¶2). Using SSL alone does not guarantee that the website is legitimate. The best way to make sure the website is legitimate is to go to directly to the real company’s website via your web browser by typing the url into the address bar in a new browser window. For example, if you received a phishing email from Paypal claiming that your information needs to be updated, then you should go directly to the Paypal website by entering http://www.Paypal.com into a new web browser window, ignoring any links in the body of the email. If the email is truly from Paypal, then they will reflect this status on their website, which will prove to you one way or the other the legitimacy of the suspected email. You should always remember that no self-respecting company will ever ask for personal information via email (Doyle, 2005, ¶14). Being cautious and aware are very important. Always be suspicious until you have proof that the email is legitimate.

How do we prevent these phishing attempts from occurring? There are many software packages available for companies that will attempt to filter and divert this type of fraudulent email from ever reaching your inbox. Perhaps the first and most important action you can take to prevent your email from receiving phishing emails is to refrain from posting your email address on bulletin boards, forums, advertisements, and other publicly viewable places that email harvesting software can easily grab them from. While most are gathered in this way and by the use of random generators, some are gathered from stolen databases from companies. While there is little you can do once your information has been stolen, you can use the techniques
demonstrated here to stop the emails once you receive them, and hopefully prevent them before you receive any!

While phishing, a technique that relies on spam email, embedded links, and fraudulent websites to accomplish identity theft, is becoming more and more prevalent, hackers are increasingly turning to pharming, which exploits security problems in peer-to-peer software and the internet's Domain Name Services (DNS) (Korzeniowski, 2005, ¶1). Specifically, this type of attack relies on a more technical aspect to do its damage. Rather than relying on the user to trust the content in an email, it operates via compromised systems or direct attacks on the DNS system. Users’ browsers reflect that they are at a legitimate website, which makes pharming somewhat more serious and difficult to detect than it’s phishing counterpart (Webopedia.com, 2005, ¶1).

The first method of attack, using compromised systems, occurs when the attacker uses peer-to-peer applications and other related software to aid in planting a Trojan horse, virus, or other destructive program and lodge it in the background of a computer (Korzeniowski, 2005, ¶3). The harmful program then locates the host files in the computer's operating system and creates an ip address for a fraudulent website that is designed to look similar to a legitimate site from a bank or credit card company, etc (Korzeniowski, 2005, ¶3). When a user types the bank or credit card company's url into his/her browser, the spyware bypasses the DNS search for the address and inserts the fake target (Korzeniowski, 2005, ¶3). In this way, a user’s home or business pc can become infected, opening the door for browser hijacking, and other forms of malicious attacks. The procedure just explained describes how the use of peer-to-peer software can enable attackers to plant programs on a user’s machine which can then alter the settings of the machine. When the user types in the url of a legitimate site, such as http://www.Ebay.com, everything seems normal, but the spyware lodged in the computer invisibly redirects the user to an exact copy of
Ebay.com. Just by looking at the site, it appears that all is well, but in fact, the user is logging into a fraudulent site. I have had first-hand experience with this as well, where lab computers used by students to check their email were so infected with spyware and adware that many important pages were redirected to either advertising pages or other sites that loaded even more malicious code to the system. One was infected with over 700 different types of spyware and adware! It’s definitely unwise to log into anything via machines in this condition, yet students were logging in as if nothing was wrong, then wondering why their accounts were being used to send emails they had never sent! This demonstrates the need for awareness among computer users on the dangers of ignorance.

This proves another important point as it relates to security: without physical security, there is no security. By restricting who has access to the pc, via the room the pc is located in, as well as over the network, you can drastically limit the chances of someone infecting or modifying your system. Another personal experience related to this that was not directly due to a system compromise, originated from just looking at a fake website sent to me in an email. I clicked on the link, which claimed to be from Suntrust, and was redirected to a website that looked exactly like the genuine website, because it was loading the pictures directly from the real site! This fraudulent website was actually loading the images from Suntrust’s servers and loading them on the fraudulent website’s page, making it almost impossible to distinguish it from the legitimate site! This was possible due to Suntrust’s permissions on their server’s folders. They allow loading of images from other locations, because they are used by Suntrust in legitimate emails, by advertising partners, etc. Personally, I feel this is just inviting attackers to abuse the content. The only real difference I noticed between the legitimate site and this fake one was that the address bar in my Internet Explorer browser was below the real address bar, and pasted over
top of part of the website area. Whoever created this fraudulent website took the time to fabricate a script that was supposed to place a little yellow lock icon and address of the format ‘https://www.suntrust.com’ on top of the real address bar. If successful, this would make it appear that the user was using a ssl secured website, but really they would be at another location. Fortunately for me, the creator of this script designed it for a browser which had more toolbars visible than mine did, and it displayed below the real address bar on my browser, showing it was a fake! Fortunately, I had no account with this online bank to begin with. This just illustrates some of the measures criminals will go to in an attempt to get your information.

So, how do you prevent this from occurring to you? The example I just described from personal experience was not due to my computer being compromised, but rather to a script loaded by the fraudulent website that attempted to ‘fake’ users into thinking they were at a legitimate site. I was aware the site was fake before I clicked on it, due to seeing the fraudulent url in the email, as discussed in the phishing section earlier in this paper. The pharming techniques caused by spyware described earlier can be prevented by ensuring your computer is free from malicious code which may allow this type of harmful software onto your computer to begin with. There are many resources available for this, the most trusted being ad-aware, spybot search and destroy, and noadware, available from http://www.lavasoftusa.com/, http://www.safer-networking.org/en/download/, and http://www.noadware.net/ respectively. A tool called spywareblaster, which prevents some spyware from ever being loaded on your system to begin with is also available at http://www.javacoolsoftware.com/spywareblaster.html. Beware of some copies of these scanners on the net, which promise to scan and clean your system, but actually plant spyware and other malware onto your system! There are lists of such software on the net.
Once again, the moral of the story is, be aware and cautious. Don’t take everything at face value, but rather wait until you have evidence to prove the email or website in question is either legitimate or fraudulent. Most fraudulent email will have the same ‘look and feel’ as the legitimate website it is imitating, so the only obvious feature that makes the phishing email stand out may be the tremendous amount of information requested (Dhamija & Tygar, 2005). It should be obvious that no legitimate company will request such things as your Social Security Number, bank account information, Paypal email and password, etc. The thing to remember is to always be aware, and always distrust emails received, until you can prove that they are indeed legitimate.

Another method which can be used by pharmers to initiate a pharming attack is by attacking the DNS system itself, either by compromising a DNS server and inserting a fake address or flooding a server and then directing traffic to a fake site (Korzeniowski, 2005, ¶3). The DNS system is the mostly transparent but extremely important part of the internet that acts like a phonebook, as it matches domain names such as Ebay.com, to ip addresses, such as 66.135.192.87. It is actually a database of all the domain names in use and their corresponding ip addresses. Without the DNS system, instead of typing ‘http://www.Ebay.com’ into your browser to go to Ebay’s website, you would have to type ‘http://66.135.192.87’ instead. The DNS system receives millions upon millions of requests each day. Without it, websites and various other nodes on the internet would become unavailable by use of their domain names. This truly is an enticing target for attackers. In addition to this, some DNS servers aren’t maintained with the latest patches and security updates that they need, making the problem worse. After an unsuspecting user arrives at a fraudulent site via this DNS vulnerability, they may enter personal data, such as credit card numbers, bank account info, or social security numbers
Most people feel fine doing this because they visited the legitimate form of the web site in the past without any problem (Korzeniowski, 2005, ¶4). As far as they know, nothing is wrong but they are actually giving their login and other sensitive information to criminals who now can use it to commit further crimes.

How can this be avoided? One of the main ways to prevent submitting information on a fraudulent site via a DNS attack is to be aware of things that may seem out of the ordinary on the web site in question. Although it may be almost impossible to tell if you are the victim of a DNS based pharming attack, some companies like Paypal and Ebay have created toolbars which load into your browser and alert you if you are on a non-legitimate website. Microsoft also has integrated an anti-phishing option into it’s ‘MSN Search’ toolbar. This works by checking the web pages that users visit with an online database that is regularly updated with information on phishing sites (Gonsalves, 2005, ¶6). If a site contains components of a phishing site, but it isn’t a confirmed threat, then the software will issue a warning and allow the option of either proceeding or avoiding the site altogether (Gonsalves, 2005, ¶6). Improving browser security to discourage the falsifying of addresses or crypto plug-ins to verify the digital certificates of websites may help (Leyden, 2005, ¶3). However, one must be aware of what is bundled with these toolbars, such as spyware or other programs that might hurt more than they help. Some ‘privacy toolbars’ in the past had malicious or advertising code embedded in them, which ultimately resulted in a slower and worse computing experience for the user than before the toolbar was installed.

If you are in charge of a DNS machine or nameserver, you can do your part in preventing this from occurring on your servers by ensuring the security patches and updates are kept up to date, and that your systems are adequately protected from attacks via the internet. A major way
to detect and deal with DNS attacks once they have occurred is by using the proper logging and auditing (Bellovin, 1995). With the explosive growth of the internet, this is becoming an increasingly attempted attack. We can all do our best to keep this type of crime from occurring, and to help the internet become a more useful and safer place to work and play.

In conclusion, the ultimate defense relating to phishing, pharming, and all other online attacks is in being aware and alert. People are the first line of defense, so an in-depth review and training into how to identify and prevent these schemes would be beneficial for any staff, individual, or employee exposed to the internet. Because people, home users and employees alike, have the ability to effectively bypass any and all security mechanisms securing their computer systems, networks, and personal data, this is a critical subject which needs to be included in any user training or awareness program. An educated user is much less likely to fall for schemes they would otherwise be figuring out for the first time, potentially playing into the hands of these online criminals. A wise motto to always keep in mind is “assume nothing and check everything” (Whitman, Mattord, 2004). Hopefully now you know some of the things to look for and have the skills necessary to do your part in helping to make the internet a safer and more efficient place to work and play.
References


Figure Captions

Figure 1. JPEG image of a phishing email I received.

Figure 2. JPEG image of encoded and decoded strings.

Figure 3. JPEG image of response from reporting the phishing email I received.

Figure 4. JPEG image of phishing email (with fraudulent link) I received.

Figure 5. JPEG image of whois information for domain of the fraudulent link I received.
Dear Friend,

I am writing you concerning my money which is presently frozen in the Bank in London due to the present condition of my family. I am Prince Taylor, the son of the former President of Liberia, President Charles Taylor who is presently on exile.

During the political crisis in Liberia, my father deposited a huge sum of money for me and my sister in a bank in London and in a private security company for safe keeping.

Right now, I need you to stand as my father's foreign business partner so that the money can be transferred to your account, so that I can start a new life, a new business with my sister.

All the legal documents that my father used to deposit this money in the Bank and the security company are with me. Please, I want this to be confidential because nobody knows that I am presently seeking asylum in Ghana.

Please, I am ready to give your percentage of the whole money with some gold and diamonds if you show assistance to my condition.

I will be expecting your response as soon as possible.

Yours sincerely
Prince Taylor
<table>
<thead>
<tr>
<th>Encoded String</th>
<th>Decoded String</th>
</tr>
</thead>
<tbody>
<tr>
<td>=6B=79=20=54=61=79=6C=6f=72?=</td>
<td></td>
</tr>
</tbody>
</table>
Dear sir or madam,

Thank you for informing us this matter.

This account is terminated.

Best Regards,
Ohad Harei-Walla! Abuse Team.
Dear PayPal Member,

PayPal is committed to maintaining a safe environment for its community of buyers and sellers. To protect the security of your account, PayPal employs some of the most advanced security systems in the world and our anti-fraud teams regularly screen the PayPal system for unusual activity.

Recently, our Account Review Team identified some unusual activity in your account. In accordance with PayPal's User Agreement and to ensure that your account has not been compromised, access to your account was flagged. Your account will remain flagged until this issue has been resolved. This is a fraud prevention measure meant to ensure that your account is not compromised.

In order to secure your account and quickly restore full access, we may require some specific information from you for the following reason:

Our system requires further account verification.

Case ID Number: PP-056-245-481 We encourage you to log in and restore full access as soon as possible. Should your account remain flagged for an extended period of time, it may result in further limitations on the use of your account or may result in eventual account closure.

Please click on the link below to log in and restore full access to your account.

Click here to activate your account [link to: http://www.pay.com/uk/ingp/paypal/confirm.html]

Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your account. We apologize for any inconvenience.
Registrent:
Yang Memorial Methodist Social Service
54, Waterloo Road, Kowloon
HK

Domain Name: YANG.ORG.HK

Record last updated on 2005-01-20
Record created on 1999-10-29
Record expired on 2006-01-22

Administrative Contact:
Kelvin Chan kevinchan@yang.org.hk
Yang Memorial Methodist Social Service
54, Waterloo Road, Kowloon
HK
+852--22510840
+852--27701417

Technical Contact:
Administrator Domain-Name domreg@ithome.net
ITHome Ltd.
P.O.Box. 73103 Kowloon Central Post Office Kowloon
HK
+852--8101 1573
+852--8101 2202