Understanding Cyber Criminals Multifaceted Techniques for Phishing and Pharming

A. E. Durosinmi
Information & Communication Technology Unit
Federal Medical Centre Abeokuta, Ogun State. Nigeria.
&
DOTS Institute of Technology, Abeokuta, Ogun State.
cunlexie@hotmail.com

Abstract
The challenges associated with the phishing & Pharming problems are presente. Their typologies are also identified and recommendations on how both can be mitigated are proferred.

Keywords: Phishing, fraud, detection, E-mail, Pharming

1.0 INRODUCTION

Phishing is the combination of social engineering and technical exploits designed to convince a victim to provide personal information, usually for monetary gains to the attacker (Phisher). Phishing scams can happen when malicious organizations or people (also known as cybercriminals) present themselves as an entity users can trust, then try to trick them into providing personal information. Phishing scams normally occur via emails, websites, text messages and phone calls that can delude recipients' to think that Christmas came early. Cybercriminals will often pose as your bank or financial institution, your employer, or any other entity that you normally trust with your information. Only when the email phishing process and characteristics are fully understood can effective measures be designed against phishing attacks. Successful phishing attacks are based on a form of copying, or reengineering, a website's design and layout in order to pass themselves off as a genuine (targeted) website.

A malicious website is crafted which looks and feels like the original site, convincing unsuspecting users that they are giving personal information to a trusted organization [1]**.** Users are frequently drawn to the sites by forged emails designed to look like legitimate correspondence and may even copy the body from real email, but when the user clicks a link to visit the website, they will be directed to the malicious site instead. The more convincing a phishing attack appears - or rather, the more genuine a malicious website looks - the more success the attack will have in extracting personal information. Some phishing attacks go so far as to create faux websites for which there is no legitimate counterpart; e.g. a page prompting users for personal information the organization wouldn't have otherwise asked for.

Before delving further into phishing it's important to clarify what is not phishing. Nigerian 419scam (sending emails to trick recipients into giving money to the scammer) and Internet auction1 fraud (non-delivery, misrepresentation, fee stacking, or selling stolen goods) are not considered phishing since they don't involve obtaining users' credentials. The latest statistics reveal that banks and financial institutions along with the social media and gaming sites continue to be the main focus of phishers [2].

Some loyalty programs are also becoming popular among phishers because with them phishers can not only breech the financial information of victim but also use existing reward points as currency. U.S. remains the largest host of phishing, accounting for 43% of phishing sites reported in January 2012. Next was Germany at 6%, followed by Australia, Spain, Brazil, Canada, the U.K., France, Netherlands, and Russia. A study of demographic factors suggests that women are more susceptible to phishing than men and users between the ages of 18 and 25 are more susceptible to phishing than other age groups. Phishing attacks that initially target general consumers are now evolving to include high-profile targets, aiming to steal intellectual property, corporate secrets, and sensitive information concerning national security [2].

Pharming is an attack on network infrastructure that results in a user being redirected to an illegitimate website despite the user having entered the correct web address. Such attacks succeed by exploiting weaknesses in the core technologies and processes that underpin the operation of the Internet. Both phishing and pharming are increasingly used not only to trick targets into revealing personal information, but also as a technique for installing malicious software (malware) [11].

1.1 Steps In Phishing Attack

All phishing attacks fit into the same general information flow. At each step in the flow, different countermeasures can be applied to stop phishing. [6]

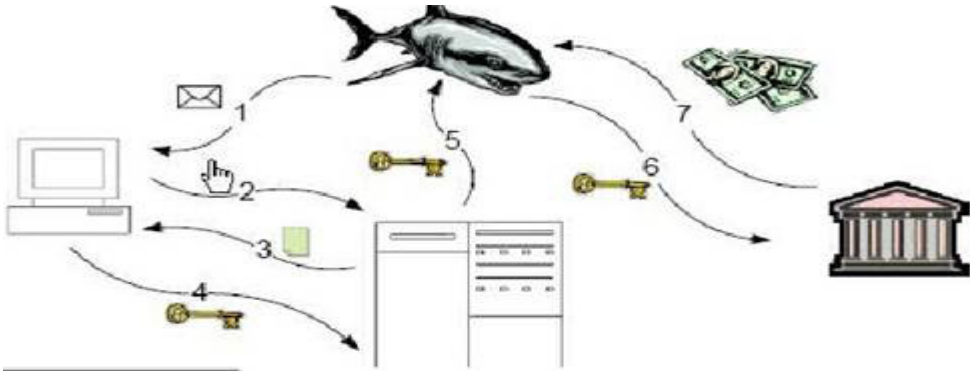


Fig. 1: Typical Phishing Scenario
http://www.scribd.com/doc/12620374/Phishing-Attack-Countermeasures

The steps are:

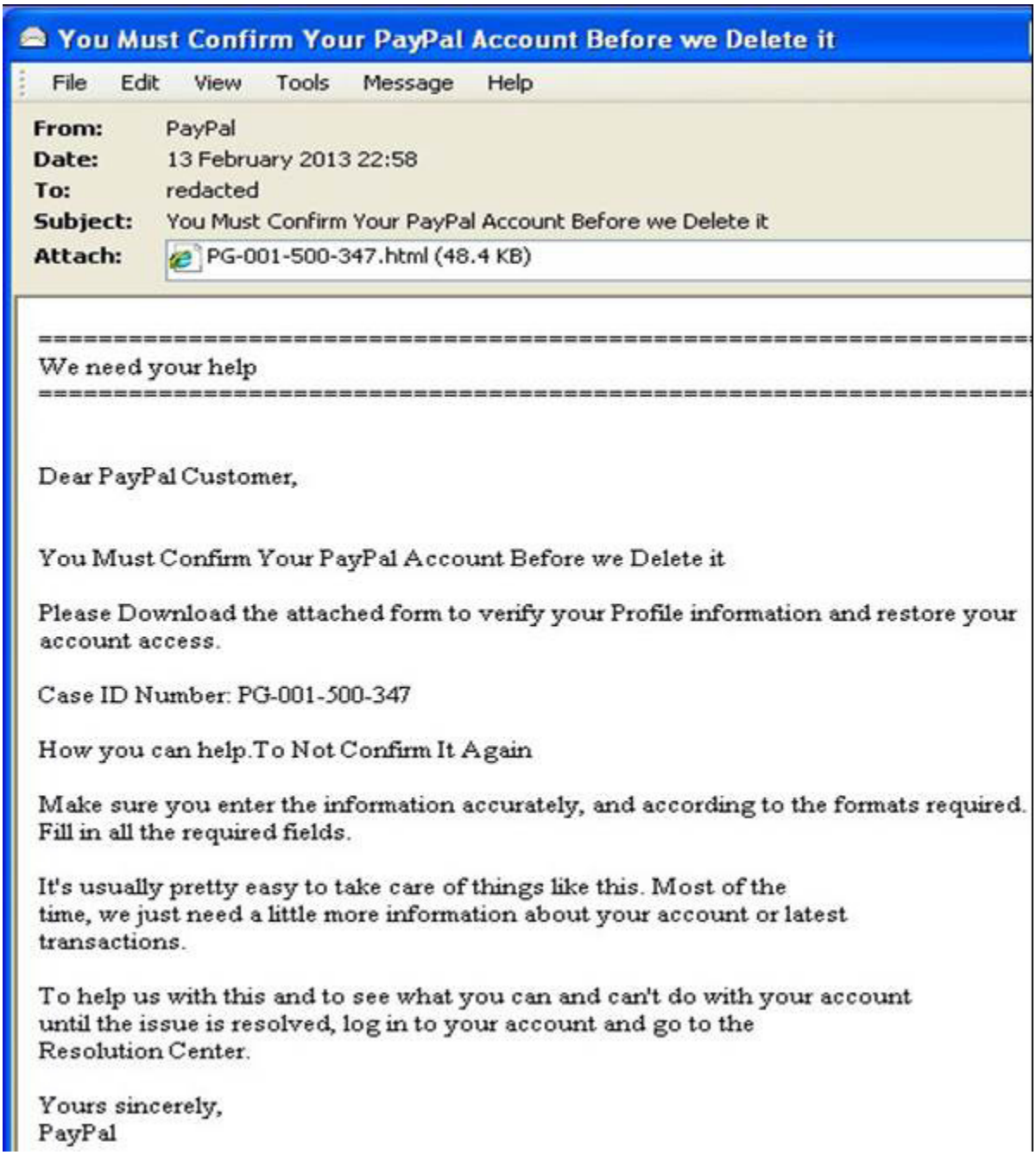
1. The phisher prepares for the attack. Step 0 countermeasure include monitoring malicious activity to detect a phishing attack before it begins
2. Malicious payload arrives through some propagation vector. Step 1 counter measures involve preventing a phishing message or security exploit from arriving.
3. The user takes an action that makes him or her vulnerable to an information compromise. Step2 countermeasures involve detecting phishing tactics and rendering phishing messages less deceptive.
4. The user is prompted for confidential information, either by a remote web site or locally by a Web Trojan. Step 3 countermeasures are focused on preventing phishing content from reaching the user.
5. The user compromises confidential information .Step 4 counter measures concentrate on preventing information from being compromised.
6. The confidential information is transmitted from a phishing server to the phisher. Step 5 countermeasures involve tracking information transmittal.
7. The confidential information is used to impersonate the user. Step 6countermeasures center on rendering the information useless to a phisher.
8. The phisher engages in fraud using the compromised information. Step 7countermeasures focus on preventing the phisher from receiving money

2.0 PHISHING TYPES &TECHNIQUES

There are a number of different phishing techniques used to obtain personal information from users. As technology becomes more advanced, the phishing techniques being used are also more advanced [3]. To prevent Internet phishing, users should have knowledge of various types of phishing techniques and they should also be aware of anti-phishing techniques to protect themselves from getting phished. Let's look at some of these phishing techniques.

2.1 Email Phishing

Phishers may send the same email to millions of users, requesting them to fill in personal details. These details will be used by the phishers for their illegal activities. Phishing with email and spam is a very common phishing scam. Most of the messages have an urgent note which requires the user to enter credentials to update account information, change details, and verify accounts. Sometimes, they may be asked to fill out a form to access a new service through a link which is provided in the email [3]



You Must Confirm Your PayPal Account Before we Delete it

File Edit View Tools Message Help

From: PayPal
Date: 13 February 2013 22:58
To: redacted
Subject: You Must Confirm Your PayPal Account Before we Delete it
Attach: PG-001-500-347.html (48.4 KB)

==========

We need your help

==========

Dear PayPal Customer,

You Must Confirm Your PayPal Account Before we Delete it

Please Download the attached form to verify your Profile information and restore your account access.

Case ID Number: PG-001-500-347

How you can help.To Not Confirm It Again

Make sure you enter the information accurately, and according to the formats required. Fill in all the required fields.

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account or latest transactions.

To help us with this and to see what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

Yours sincerely,
PayPal

The spam message itself was what you expect - social engineering being used in an attempt to trick the recipient into opening the attachment.

If the user opens the attachment, they are presented with what looks to be a PayPal login page. Inspection of the HTML source confirmed that the various forms within the page referenced legitimate PayPal resources.
The page did load suspicious JavaScript content from a non-PayPal server however. Furthermore, there was a suspicious (or at least unexpected) empty frame within the page.

```
</div>
<!-- END BILLING PAGE -->
<iframe id="target" src="#" style="visibility: hidden;">
</iframe>
```

The remote JavaScript revealed the key to how the attack worked. The script was being used to validate user input entered into the various PayPal forms.
Data from the customer signup form was serialized and stored in the variable cus_data.

Then, data from the subsequent billing form was also serialized, and stored in the variable cc_data.

These variables were then sent back to the attackers by dynamically populating the empty frame element (see above).

```
submitHandler: function(form, validator) {
    cc_data = $(form).serialize();

    $(form).find('#messageBox').hide();

    $('#target').attr('src', data_receiver_url+'?'+cus_data+'&'+cc_d
    $('#target').load(function(){
        document.location.href = redirect_url;
    });
},
```

Cunning! So by hooking the form submission process, and then dynamically populating the frame, the attackers are able to send the form data back to their server. This included all of the following:

- Email
- Password
- First name
- Last name
- Date of birth
- Citizenship
- Address
- Telephone number
- Credit card number
- Cvv number
- Expiry date
- Sort code
- Social security number
- Customer id

So why bother with all this? Why not stick to the basics and just edit the target of the HTML form?

There are probably two advantages to the technique used in this attack:

1. The spammed web page will raise less suspicion. Seeing forms pointing to unexpected remote servers is a giveaway sign of the page being a phish.
2. The mechanism enables them to include data from multiple forms. Ideal for complex sites where customers may enter data in different steps [9].

2.2 Web Based Delivery

Web based delivery is one of the most sophisticated phishing techniques. Also known as "man-in-the-middle," the hacker is located in between the original website and the phishing system. The phisher traces details during a transaction between the legitimate website and the user [3]. As the user continues to pass information, it is gathered by the phishers, without the user knowing about it.

2.2.1 Fake Banner Advertising

Banner advertising is a very simple method Phishers may use to redirect an organisations customer to a fake web-site and capture confidential information. Using copied banner advertising, and placing it on popular websites, all which is necessary is some simple URL obfuscation techniques to obscure the final destination [10].

With so many providers of banner advertising services to choose from, it is a simple proposition for the Phisher to create their own online account (providing a graphic such as the one above and a URL of their choice) and have the service provider automatically distribute it to many of their managed websites. Using stolen credit cards or other banking information, the Phisher can easily conceal their identity from law enforcement agencies [8].

3.0 PHISH & LEGITIMATE EMAIL

Phishers are targeting the customers of banks, online payment services and social networking sites like HSBC Bank, PayPal, Fedex, Facebook, Evernote, Twitter and LinkedIn etc. Users of any online service or social networking site can be targeted through phishing emails and scams in a number of ways through emails. Below will show you how you can easily recognize a phishing email, just **through hovering with your mouse** and applying some common sense. It is easy once you know what to look out for. Phishing emails are one of the most common ways for fraudsters to scam unsuspecting consumers. LinkedIn has certainly become one of the most popular business-to-business social networking tools, some even say the site is replacing recruitment sites! Not surprisingly, it is becoming a target for phishing attempts. This email, which masquerading as a member invitation from popular business focused social network LinkedIn, recipients are asked to click on a link 'visit your Inbox now' to view the pending messages [4]

The email includes the LinkedIn logo and looks very similar to a genuine LinkedIn invitation message. However, the message is not from LinkedIn. All of the links in the message lead to compromised websites that have no connection to LinkedIn. BlackHole is a web application used by criminals to exploit browser vulnerabilities as a means of downloading and installing Trojans and other types of malicious software into victim's computer. If an email contains a link and you're unsure whether it's legitimate, hover over it with your mouse to see what address it directs you to. To avoid being scammed read the below guide how to spot a scam and protect yourself from such type of phishing attacks [3] [5]

3.1 LinkedIn Phishing

In fact, LinkedIn has regularly been targeted in such malware and phishing attacks. Always ensure that LinkedIn messages are really from LinkedIn. Scam emails often use HTML to disguise links in their bogus messages. As you can see below screen shot, this email looks somewhat credible. However, we can differentiate LinkedIn phishing email from a real LinkedIn email from the below screen shot:

A LinkedIn Phishing Email

The message body says:
LinkedIn Reminders
Invitation Reminders:
From Akshay Das (Senior Director, Business Development, Information & Media Division at The McGraw Hill Companies.)
Pending Messages
There are a total of 3 messages awaiting your response. Go to Inbox now (clickable link to malicious site) Take a look at the **From** Field in the screenshot; you can see that the mail is not originally coming from LinkedIn.

The highlighted text that states '**go to inbox now'** does not pointing to a true LinkedIn website.

Fig. 3: LinkedIn Phising Scam

In summary, the sender is not LinkedIn, hovering over the clickable links reveals that the urls are not LinkedIn, but pointing to a Russian domain.A quick search will reveal that McGraw Hill Companies is real, and there are several people named Akshay Das on the LinkedIn network, but none appear to work for McGraw Hill. The scammers have used a real company and a real name to give their scam more credibility.

3.2 A Real LinkedIn Email

As you see in the real email from LinkedIn, the url pointing to LinkedIn website itself.

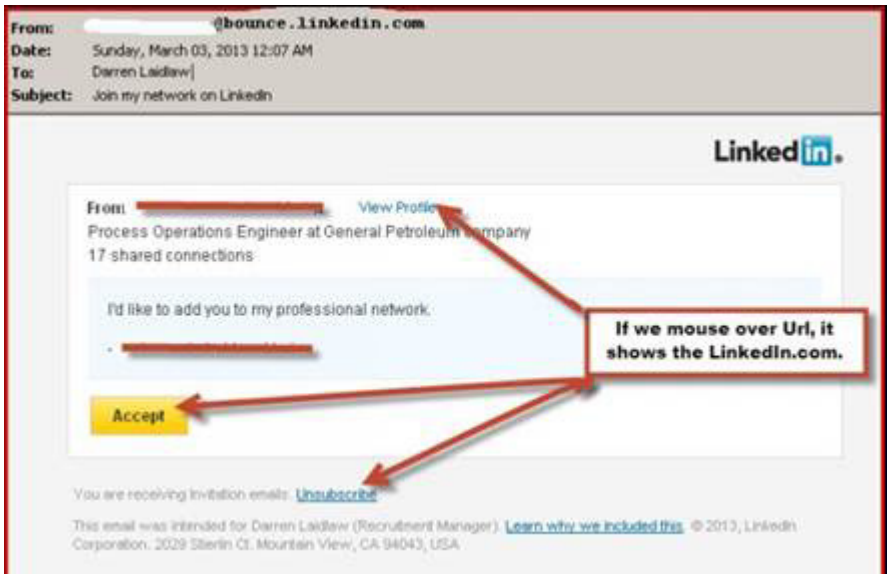


Fig. 4: Real LinkedIn Email

The From Field in the screenshot tells you that the email is from ….@bounce.linkedin.com – a real LinkedIn email address.

The links in the screenshot shows the linkedin.com domain in the URLS when you hover over them with the mouse.

The Email Source
We would like to share the source code behind both the real and phishing emails.
Source code of the fake LinkedIn email:
You can see that the URL hiding in the code is http ://doctormusi.ru/templates/beez/track. php?c002 you see there is a tracking

```
<h1 style="margin: 5px 0px; color: #000000; font-weight: bold;">LinkedIn</h1>
<h2 style="margin: 0px; padding: 0px; color: rgb(0, 102, 153);">REMINDERS</h2>
<p style="margin: 10px 0px; font-size: 12px;"><strong>Invitation reminders:</strong></p>
<span></span> From <strong><a href="http://doctormusi.ru/templates/beez/track.php?c002"
```

code at the end. Tracking codes are strings of text added to the end of a URL which let you track the source of a click.
Source code of the real LinkedIn email:

```
<table cellpadding="0" cellspacing="0">
  <tr>
      <td style="width:15%; padding-right:20px;">
                                                  <table bo
      </td>
      <td style="font: 13px arial, sans-serif;">
          <a href="http://www.linkedin.com/e/9lm04f-
      </td>
  </tr>
</table>

<br>
```

You can see that the URL hiding in the code is http://www.linkedin.com, so clicking on links in real emails from LinkedIn is safe.

Phishing scams of this nature are all too common and, in spite of widespread publicity, they continue to fool people all around the world into handing over their financial and personal information. Legitimate banks and other financial institutions will never send their customers unsolicited, generic emails that request them to click a link to login and provide personal information.

4. MITIGATING PHISING

In order to mitigate phising attacks, it is important for users to deny requests that asked them to supply personal information directly into the e-mail or submit via online. Other such requests to be rejected include any mail or requests that:

- Threatens to suspend or close your online accounts if you do not respond for the email.
- Claims that your account has been compromised or accessed by un authorized person.
- Requests you to enter, validate or verify your account information.
- States that there are unauthorized charges on your account and requests your account information.
- Claims that the bank has lost important security information and needs you to update your information online.
- Requires you to enter your card number, password, user ID or account numbers into an email.

The following can also be done in addidtion to what has been mentoioned earl;ier:

- Never click on Hyperlinks within emails, instead, copy and paste them into your browser.
- Do not open any file attached to the email.
- Always look for “https://” and padlock on web sites that require personal information.
- If you didn’t initiate a transaction to which an email is referring, it’s probably a scam.
- Never respond to spam / suspicious email or emails from unknown senders.
- Do not supply your personal / Bank account information to strangers, they are most likely scammers.
- Use spam filtering software.

5. CONCLUDING REMARKS

In this paper, i x-rayed phishing in its many guises. Using concrete examples, i showed how e-mail phishing scams can be used to defraud unsuspecting users. I also revealed that phishing scams can occur via email, websites, text messages, and sometimes phone calls. I embellished the phishing and pharming scenario in order to provide some understanding to electronic mailing systems and online consumers that can serve as a bases for empowering users and organization in their quest to mitigate phishing attacks.

REFERENCES

[1] Approaches to Phishing Identification Using Match and Probabilistic Digital Fingerprint Techniques. http://www.mcafee.com/us/resources/white-papers/wp- approaches-to-phishing-identification.pdf

[2] Phishing.http://www.cs.arizona.edu/~collberg/Teaching/466566/2012/Resources/presentations/2012/topic5-final/report.pdf

[3] Phishing Techniques. http://www.phishing.org/phishing-techniques/

[4] LinkedIn Phishing Emails – How to distinguish between a Phish and a Legitimate Email, March 5, 2013. Available at: http://omniquadsecurityblog.com/2013/05/20/omniquad-warns-fake-speeding-ticket-emails-carry-w32-fakehddrepair-trojan/

[5] http://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Trojan:Win32/FakeSysdef

[6] Harish, 'Phishing Attack & Countermeasures', Feb 19, 2009. Available at: http://www.scribd.com/doc/12620374/Phishing-Attack-Countermeasures

[7] Fraser Howard', 'Spicing up phishing attacks' on March 27, 2013. Available at: http://nakedsecurity.sophos.com/2013/03/27/spicing-up-phishing-attacks/

[8] http://www.technicalinfo.net/papers/Phishing.html

[9] Fraser Howard, 'Spicing up phishing attacks', March 27, 2013. Available at: http://nakedsecurity.sophos.com/2013/03/27/spicing-up-phishing-attacks/

[10] Gunter ollmann, 'The Phishing Guide (Part 1) Understanding and Preventing Phishing Attacks', Available at: http://www.technicalinfo.net/papers/Phishing.html

[11] http://www.cpni.gov.uk/Documents/Publications/2010/2010019-Phishing_pharming_guide.pdf