Techniques of Preventing Computer Crime on Phishing

Prof. Kartikbhai Baldevbhai Patel

Asst. Prof., Department of MCA, Smt. K. K. Patel MBA/MCA College, P.O: Palasar, Nr. Shelavi Railway Station, Taluka: Chanasma, Dist: Patan[N.G.],Gujarat, India
Affiliated to Gujarat Technological University, Ahmedabad

ABSTRACT:
Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legal one. Phishing has become the fastest growing scam on the Internet. Phishing Techniques main aims are for preventing the crime on computer.

Phishing (password + fishing) is a form of cyber crime based on social engineering and site spoofing techniques. The name of ‘phishing’ is a conscious misspelling of the word ‘fishing’ and involves stealing confidential data from a user’s computer and subsequently using the data to steal the user’s money. In this paper, we study, discuss and propose the phishing attack stages and types, technologies for detection of phishing web pages, and conclude our paper with some important recommendations for preventing phishing for both consumer and company.

Only one tool was able to consistently identify more than 90% of phishing URLs correctly; however, it also incorrectly identified 42% of legitimate URLs as phish. Thus we demonstrate that the source of phishing URLs and the freshness of the URLs tested can significantly impact the results of anti-phishing tool testing. We also demonstrate that many of the tools we tested were vulnerable to simple exploits.

Keywords: Phishing prevention techniques for security attack.

[1] INTRODUCTION

The phishing techniques are to decrease the less spoofing attack on web and prevent the crime on computer so gathering more prevention techniques for security attack.

Banks and other organizations deal with fraudulent phishing websites by pressing the hosting service providers to remove the sites from the Internet. Until they are removed, the fraudsters will learn the passwords, personal identification numbers (PINs) and other personal details of the users who are fooled into visiting them. We analyze empirical data on actual phishing website removal times and the number of visitors that the websites attract, and conclude that website removal is part of the answer to phishing, but it is not fast enough to completely mitigate the problem.

[1.1] WHAT IS PHISHING?
Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legal one. Phishing has become the fastest growing scam on the Internet.

'Phishing' refers to emails, sent to you by scammers, which are designed to trick you into providing your personal and banking information.

Typically, scammers will send phishing emails which often appear to be from your bank, a government organization, a company or other financial institutions urging you to click on a link to update your personal profile or 'validate' or 'confirm' your personal details.

Phishing is a kind of amalgamation of Web technology and social engineering. The most popular phishing scams are carried out using phishing web pages. Phishing web pages are forged to mimic certain legitimate companies’ web pages. Phishing websites usually trick users into Leaking their sensitive information and private data by counterfeiting trustworthy web identities.

Phishes can simply download targeted web pages from the real websites and put them onto the phishing websites.

[1.2] TYPE OF PHISHING

1. **Misspelled URLs**: Phishers use some sort of deceptive techniques, which design a link in an e-mail (and the spoofed website it leads to) apparently belong to the spoofed organization by using misspelled URLs or of sub-domains. Sometimes the phishers make the anchor text for a link appear to be valid, whereas the link actually goes to the phishers site.
2. **Whaling**: Phishing attacks directed specifically at senior executives and other high profile targets within businesses is known as Whaling.
3. **Image Phishing**: Phishers have also used images instead of text to make it difficult for anti-phishing filters.
4. **Cross site scripting**: An attacker can even exploit flaws in the original website’s script against the victim making it even more difficult to detect since everything from the web address to the security certificates seem to be original. This technique is known as cross site scripting.
5. **Phone Phishing**: Phone Phishing is the case where in a customer gets a call asking him to call back to discuss his problems while accessing his bank accounts. The person then is trapped into giving his sensitive information such as credit card information and the like.
6. **Spam e-mail**: spoofed to look like correspondence from a legitimate financial institution.
7. **Hostile profiling**: a targeted version of the above method: the cyber criminal exploits web sites that use e-mail addresses for user registration or password reminders and directs the phishing scam at specific users (asking them to confirm passwords, etc.).
8. **Install a Trojan:** that edits the hosts file, so that when the victim tries to browse to their bank’s web site, they are re-directed to the fake site.

9. **Spear phishing:** an attack on a specific organization in which the phisher simply asks for one employee’s details and uses them to gain wider access to the rest of the network. For traditional phishing sites, removing either the hosting website or the domain (if only used for phishing) is sufficient to remove a phishing site.

**[1.3] HOW PHISHING WORKS?**

Suppose you check your e-mail one day and find a message from your bank. You've gotten e-mail from them before, but this one seems suspicious, especially since it threatens to close your account if you don't reply immediately. What do you do?

This message and others like it are examples of phishing, a method of online identity theft. In addition to stealing personal and financial data, phishers can infect computers with viruses and convince people to participate unwittingly in money laundering.

From beginning to end, the process involves

1. **Planning.** Phishers decide which business to target and determine how to get e-mail addresses for the customers of that business. They often use the same mass-mailing and address collection techniques as spammers.

2. **Setup.** Once they know which business to spoof and who their victims are, phishers create methods for delivering the message and collecting the data. Most often, this involves e-mail addresses and a Web page.

3. **Attack.** This is the step people are most familiar with -- the phisher sends a phony message that appears to be from a reputable source.

4. **Collection.** Phishers record the information victims enter into Web pages or popup windows.

5. **Identity. Theft and Fraud.** The phishers use the information they've gathered to make illegal purchases or otherwise commit fraud. As many as a fourth of the victims never fully recover

---

![Phishing Diagram](image-url)
If the phisher wants to coordinate another attack, he evaluates the successes and failures of the completed scam and begins the cycle again.

Phishing scams take advantages of software and security weaknesses on both the client and server sides. But even the most high-tech phishing scams work like old-fashioned con jobs, in which a hustler convinces his mark that he is reliable and trustworthy. Next, we’ll look at the steps phishes take to convince victims that their messages are legitimate.

**[2] PHISHING ATTACK CLASSIFICATIONS**

The most popular phishing strategies can be classified as web page obfuscation and/or Web link obfuscation

**[2.1] WEB PAGE OBFUSCATION**

Web page obfuscation can be carried out in two basic ways,

- Use the downloaded web Pages from real websites or create similar web pages to make them appear and react similar to the real ones;
- Use graphical components rather than HTML to avoid HTML based phishing detection, e.g. the graphical components could be Java Script, ActiveX, Macromedia Flash, Java Applet, and Image, They can be used to create visually identical web pages as well.

**[2.2] WEB LINK OBFUSCATION**

Web link obfuscation can be carried out in five basic ways,

- Add prefix or suffix to Domain name to generate faked URL, such as www.citibank.com.info123.com;
- Use Actual links which are different from the visible ones, e.g. <a href="phishing.htm"> Citibank</a>;
- Utilize website bugs to redirect the link to the phishing web pages, e.g. http://www.google.com/url?sa=U&start=4&q=http://www.mit.edu/~ayf can be redirected To a webpage other than Google;
- Use cousin domain names (e.g., to replace certain Characters in the target URL with similar characters), e.g. use www.1CBC.com (“1” is number one) to mimic www.ICBC.com (“I” is upper case “I”);
- Use Java Script or ActiveX components to mimic or cover the address bars to make users believe they have Entered the correct websites.

**[3] PHISHING TECHNIQUES**

**[3.1] PHISHING THROUGH COMPROMISED WEB SERVERS**
Most phishing attacks that we have observed in the wild involve attackers breaking in to vulnerable servers and installing malicious web content. Honey net technology allows us to capture in detail the typical life cycle of a phishing attack, and in general terms the flow of events we have observed during such incidents are as follows:

- Attackers scan for vulnerable servers
- Server is compromised and a root kit or password protected backdoor installed
- Phishers gain access to the server through this encrypted back door
- If the compromised server is a web server, pre-built phishing web sites are downloaded
- Some limited content configuration and web site testing is performed (potentially revealing the hasher’s true IP address when they first access the web server)
- Mass emailing tools are downloaded and used to advertise the fake web site via space mail.
- Web traffic begins to arrive at the phishing web site and potential victims access the malicious content.

![Figure: 2. Phishing through compromised web server](image)

Often the time taken for this incident life cycle is only a matter of hours or days from when the system is first connected to the Internet, and our research suggests that such activity is taking place on many servers and targeting many organizations at once. We will illustrate these theories using data recorded during two incidents that are typical of common phishing attacks, using one incident observed by the German Honey net Project and one incident observed by the UK Honey net Project. In each case, vulnerable Linux honeypots were deployed by Honey net Research Alliance members.

### [3.2] PHISHING THROUGH PORT REDIRECTION

On January 11th 2005, an attacker did successfully compromise the honeypot, using an exploit for the Open SSL SSLv2 Malformed Client Key Remote Buffer Overflow Vulnerability present in the default Red hat Linux 7.3 distribution. This incident was unusual in that once the attacker had gained access to the compromised system no phishing content was uploaded directly. Instead, the attacker installed and configured a port redirection service on the honeypot.
This port redirection service was designed to re-route HTTP requests sent to the honeypot web server to another remote web server in a transparent manner, potentially making the location of the content source harder to trace. The attacker downloaded and installed a tool called redirect on the honeypot, which was a port redirector utility designed to transparently forward incoming TCP connections to a remote destination host. In this incident the attacker configured the tool to redirect all incoming traffic on TCP port 80 (HTTP) of the honeypot to TCP Port 80 (HTTP) on a remote web server in China. Interestingly, the attacker did not bother to install a root kit to hide their presence on the honeypot, which suggests that the attacker did not value the compromised server too highly and that they were not particularly worried about being detected.

The command used by the attacker to establish port redirection was:

```
Redir--lport=80 --laddr=<IP address of honeypot> --cport=80 --caddr=221.4.XXX.XXX
```

Within a period of about 36 hours, 721 unique IP addresses were redirected, and once again we were surprised by how many users were apparently being tricked into accessing such content through phishing emails. An analysis of the IP addresses accessing the port redirector honeypot can be found here (note that this information has been sanitized to protect the users who accessed the phishing content, and again only IP data was logged during this research).

### [3.2] PHISHING USING BOTNETS

The recent white paper by the Honey net Project called "KYE: Tracking Botnets" introduced a method to track botnets. A botnet is a network of compromised computers that can be remotely controlled by an attacker. Due to their immense size (tens of thousands of systems can be linked together), botnets can pose a severe threat to the community when used for Denial-of-Service (DoS) attacks. Initial research in this area demonstrated that botnets are sometimes used to send out spam emails and can also be used for phishing attacks.
During a study in October 2004, email security company Cipher Trust suggested that 70% of monitored phishing spam was sent through one of five active botnets, but our own observations suggest that many more botnets are in use for spam operations. Although not the analysis of one single incident, in this section we present our observations on the tools and techniques used by attackers engaged in phishing via botnets.

[4] PHISHING ATTACKS

The phishing attack, targeted at Standard Banks’ customers, initiated from unsolicited emails, requesting a verification of email address by clicking the URL contained in the email. The link was ultimately the means to dupe customers into divulging their sensitive credentials, such as card number, password and customer selected pin. This phishing attack differs from traditional phishing attacks, as it displayed the legitimate Standard Bank web page (www.standardbank.co.za/site/about/index.jsp), and produced a pop-up screen after 5 to 10 seconds requesting customers to enter sensitive credentials. The pop-up screen overlaid Standard Bank’s legitimate web page thereby making the request seem authentic. The pop up logon screen was embedded in the URLreference. Once credentials were submitted to the pop up screen, it was transmitted to the perpetrators site. This attack was similar to the one FNB endured on the 17th of May 2005 differing in that the FNB attack was through a spoof site emulating FNB’s web page

Following two is the phishing Attacks

1. Scams
2. Facebook Phishing Attack

[4.1] SCAMS

Phishing scams attempt to trick people into providing sensitive personal information such as credit card or banking details. In order to carry out this trick, the phishing scammers send a fraudulent email disguised as an official request for information from the targeted company. Generally, they also create a “look-a-like” website that is designed to closely resemble the target company's official site. The fake website may appear almost identical to the official site. Style, logos, images, navigation menus and other structural components may look the same as they do on the genuine website.

Recipients of the scam email are requested to click on an included hyperlink. Clicking this link will cause the fake website to open in the user's browser. Once at this fake website,
the user may be presented with a web form that requests private information such as credit card and banking details, and other account data such as a home address and phone number. Often, the visitor is requested to login using his or her username and password. All information entered into this fake website, including login details, can subsequently be collected and used at will by the criminals operating the scam.

The following examples of phishing:

- **Ebay phishing email**: Perpetrator likes to send email by using eBay logo to gain credibility and cheated that billing is out of order and required eBay member to login and verify the charges again. From that, they can tries to steal sensitive personal information. Below is the example of the eBay phishing email:

  ![Figure: 5. eBay phishing email](image)

- **PayPal phishing scams**: In the example below, this PayPal phishing scams tries to cheat recipients by acting as a security alert. It claimed that someone ‘from a foreign IP address tried to login to recipient’s PayPal account and the e-mail inside include a link that urges recipients clicking it to update and confirm their account details. By clicking the link actually directs the recipient to the attacker’s website.

  ![Figure: 6. PayPal Phishing fraud](image)

- **Citibank phishing e-mail**: From the example below, we can see that the perpetrator send e-mail by acting as a safety and integrity for the online banking community to get recipient’s banking information. In the email, recipients given a
link to visit a fake website and enter banking information that the perpetrator tries to steal.

![Citibank phishing e-mail](image)

Figure: 7. Citibank phishing e-mail

### [4.1.1] PHISHING SCAMS

Phishing scams are just another attempt to get valuable information. Scammers send a mass email to every address they can find. Typically the message will appear to come from a bank or financial institution. The email states that you should update your information for one reason or another, and they usually provide a link that you can click to do so.

This all sounds reasonable and it may look legitimate, but phishing scams are anything but legitimate. The link provided does not take you to the financial institution’s website. Instead, you’ll be submitting your information to a website run by the scammers.

### [4.1.2] WHY SCAMMERS USE PHISHING SCAMS

Why would somebody do this? Well, you can gather a lot of juicy information with a phishing scam. First, you can get somebody’s account number and password. Then you can try to hijack their assets. Some phishing scams ask for all of your personal information (SSN, mother’s maiden name, date of birth, etc.) so that they can steal your identity and open credit accounts in your name. Some victims of phishing scams have given up their credit card numbers only to find that the card was used fraudulently.

### [4.1.3] WHY PEOPLE FALL FOR PHISHING SCAMS

Anybody can be tricked by a sophisticated phishing scam. Simple phishing scams are easy to spot, but the best scammers are actually pretty smart. They use a variety of tricks to make the phishing scam look like a legitimate process. For example, they might include a graphic from the bank right on the email message or website. Or, the link provided in the email may look like it goes to the bank’s website while the victim is actually sent to a very different site.

### [4.1.4] HOW TO SPOT PHISHING SCAMS
It is easy to uncover a crude phishing scam. For example, if you get an email from a bank you've never opened an account at, then don't follow the link and enter your personal information. Now, if you actually have an account at the institution it gets more interesting. You'll want to look at the message carefully to see if it is a phishing scam. Are words misspelled? Sometimes scammers operate in a second language and they give themselves away by using poor grammar.

[4.2] FACEBOOK PHISHING ATTACK

I am explaining this method first because it's the easiest and also the most popular method for hacking Facebook password. You can also search on Google the various famous Facebook hacking methods and you will find Phishing technique on the top always. And I am explaining the methods according to their popularity.

Now you want to know which my favorite method for Hacking Facebook account passwords is and I will undoubtedly tell it's simply PHISHING.

I will recommend my users to read this post for knowing how to hack Facebook using Phishing as I have explained it in detail here on my other website:

**How to hack Facebook accounts or Passwords using Phishing**

If you want latest Facebook phisher then subscribe my Hacking tricks and mail me privately or post your email below in comments. I will provide you within a day, now why I am not providing it directly, if I provide directly then Facebook will block it again like the previous one.

[4.2.1] HACKING FACEBOOK ACCOUNT PASSWORD REMOTELY USING KEY LOGGERS AND RAT'S

Best method for advanced Hackers. And my second favorite too. Its popularity is little but lower than Phishing only because it involves you to download hack tool and then create your key logger and send it to victim which is a lengthy process and also unsecured too as you don't aware that the key logger that you downloading is himself contain some spyware or simply a key logger attached with it. Key logging becomes easier if you have physical access to victim computer as only thing you have to do is install a key logger and direct it to your destination so that it will send all recorded keystrokes to pointed destination. What a key logger does is it records the keystrokes into a log file and then you can use these logs to get required Facebook password and thus can hack Facebook password.

I have written a complete article on How to hack Facebook accounts remotely using Key loggers, so i will recommend you to go through that if you want to learn this technique in detail, so read this article on my other website:

**How to Hack Facebook accounts or Passwords remotely using Key loggers**

Now if you need latest Fully Undetectable Key logger, then subscribe my hacking tricks and mail me privately or post your email ID below in comments on which you want to get the download link.

[4.2.2] HACKING THE PRIMARY EMAIL ADDRESS:

If Facebook hacker or any specific Key logger, by some means, hacks your primary Gmail or yahoo account which you are using as primary email address, then this information account can easily hack your Facebook password using "Forgot password" trick. The Hacker will simply ask Facebook to send password to the primary email address and ask Facebook administrators to send the reset email to your primary email address- which is already hacked. Thus, your Facebook account password will be reset and it will also be hacked! So, always remember to protect your primary email address that you have used to
create Facebook account and try to keep unknown or useless mail id as your primary email address in Facebook.

[4.2.3] SOCIAL ENGINEERING OR GUESSING PASSWORDS

This method sounds to be pretty not working at beginning. Even I was neglecting this way for a long time. But, once, I thought of using it against my friend on Facebook and amazingly what happened that I guessed his Facebook password very easily by this method. I think many of you might be knowing how what this social engineering, For novice hackers, Social engineering is method of retrieving password or Guessing the password or answer of security question simply be hacking some information about the victim or simply gathering his information from his own Facebook and other social networking profiles where most of users provide their critical information just for fashion and doesn't know its consequences.

[5] ANTI-PHISHING

There are a variety of methods that can be used to identify a web page as a phishing site, including white lists (lists of known safe sites), blacklists (lists of known fraudulent sites), heuristics, and community ratings. The tools examined in this study employ differing combinations of these methods. We used publicly available information provided on the tool download web sites as well as our observations to get basic understanding of how each tool functions.

![Antiphishing](Figure: 8. Anti-Phishing firewall)

[5.1] LIST OF TOOLS

Below are Anti-Phishing tools that are easily identifying Phishing crime

- **CallingID Toolbar**
- **Cloud mark Anti-Fraud Toolbar**
- **EarthLink Toolbar**
- **eBay Toolbar**
- **Firefox 2 and above**
- **GeotrustTrustwatch Toolbar**
- **Microsoft Phishing Filter in Windows Internet Explorer 7**
- **Netcraft Anti-Phishing Toolbar**
- **Netscape Browser 8.1**
- **Spoof Guard**

[5.2] ANTI-PHISHING TOOL EVALUATION

Below are Anti-Phishing tools for Evaluating Phishing crime
Manual Evaluation of Anti-Phishing Tools

Design and Implementation of an Automated Anti-Phishing Test Bed

- Step: 1 Retrieve Potential Phishing Sites.
- Step: 2 Send URL to Workers.
- Step: 3 Workers Evaluates Potential Phishing Site.
- Step: 4 Task Manager Aggregates Results.

Evaluation of Anti-Phishing Tools

[6] CONCLUSION

We conclude with our observations on tool performance, testing methodology, and user interfaces, as well as some directions for future work. Overall, we found that the anti-phishing tools that were examined in this study left a lot to be desired. Spoof Guard did a very good job at identifying fraudulent sites, but it also incorrectly identified a large fraction of legitimate sites as fraudulent. The performance of the other tools varied considerably depending on the source of the phishing URLs. Of these other tools, only IE7 was able to correctly identify over 60% of phishing URLs from both sources, but it still missed 25% of the APWG phishing URLs and 32% of the phishtank.com phishing URLs. Half the tools we tested could correctly identify less than half the phishing sites.

Many of the tools we tested were vulnerable to some simple exploits as well. Our experiments also suggest that there is no single technique that will always outperform others for identifying phishing web sites. Most of the tools we tested used blacklists, but only half of them were able to identify the majority of phishing web sites. We do not know the size of the blacklists used by each tool, nor do we know what heuristics are used by any of the tools other than Spoof Guard.

We suspect that the tools that performed best use larger and more frequently updated blacklists. They may also use heuristics that allow them to detect phishing sites that have not yet been put on their blacklist. The only tool we tested that is known to make no use of blacklists was Spoof Guard. While it was able to identify the majority of phishing sites using only heuristics, it still missed some phishing sites and it had a very high false positive rate. Spoof Guard could potentially be improved through the use of a white list, which would prevent the problems that occurred when phishing sites were visited before their corresponding legitimate sites. The white list would not necessarily need to be extremely large or updated frequently to be effective.

The success of a blacklist relies on massive amounts of data being collected at frequent intervals. Relying solely on heuristics requires that the software is designed with the foresight to prevent circumvention. In this study we were able to exploit both techniques, which lead us to believe that a combination of techniques is necessary.

REFERENCES.

Author brief Introduction:

My Self Kartikbhai Baldevbhai Patel. I currently working as a Assistant Professor (MCA Department) in Smt. K. K. Patel MBA/MCA College, Palasar, Affiliated to Gujarat Technological University.

Corresponding Address:

C/O Baldevbhai Chaturdas Patel
Jodhpur Gam,
Patel Vas,
Gomteshwer Flat Ni Gali Ma,
Satellite,
Ahmedabad,
Gujarat,
Pin code-380015.