Digital Innovations & Contemporary Research in SCIENCE, ENGINEERING & TECHNOLOGY

Vol. 5. No. 2, June., 2017

Article Citation Format
Adenekan, O.A & Durosinmi, A.E (2017):
Secure Site Identification Mechanisms in Browsers for Phishing Attacks
Journal of Digital Innovations & Contemp Res. In Sc., Eng & Tech. Vol. 5, No. 2. Pp 261-270

Article Progress Time Stamps

Article Type: Research Article
Manuscript Received: 17th May, 2017
Review Type: Blind
Final Acceptance:: 28th June. 2017
DOI Prefix: 10.22624

Secure Site Identification Mechanisms in Browsers for Phishing Attacks

[1]Adenekan, O.A & [2]Durosinmi, A.E
1&2Department of Computer Engineering
Moshood Abiola Polytechnic
Abeokuta, Ogun State. Nigeria.
E-mails: adenekanolujide@yahoo.com, cunlexie@hotmail.com

ABSTRACT

Phishing attacks cause substantial damages to individuals and corporations. We analyze these attacks, and identify that most of them exploit the fact that users are not sufficiently aware of the secure site identification mechanisms in browsers. In fact, it appears that even web designers are often confused about the need to securely identify login forms. We present the challenges associated with the phishing & security measures that service providers can take to prevent and manage a Phishing attack. In this paper, we focus on studying the structure of URLs employed in various phishing attacks.

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

1. INTRODUCTION

Phishing is form of identity theft that combines social engineering techniques and sophisticated attack vectors to harvest financial information from unsuspecting consumers. Often a phisher tries to lure her victim into clicking a URL pointing to a rogue page. We describe several features that can be used to distinguish a phishing URL from a benign one. These features are used to model a logistic regression filter that is efficient and has a high accuracy. We use this filter to perform thorough measurements on several million URLs and quantify the prevalence of phishing on the Internet today [13]. Most Internet users have encountered phishing in the form of emails purporting to come from a bank or other business, but in fact originating from a malicious source and designed to persuade the recipient to hand over personal information such as credit card details[1].

Phishing scams normally occur via emails, websites, text messages and phone calls that can delude recipients' to think that Christmas came early. Cybercriminals will often pose as your bank or financial institution, your employer, or any other entity that you normally trust with your information. Only when the email phishing process and characteristics are fully understood can effective measures be designed against phishing attacks. Successful phishing attacks are based on a form of copying, or reengineering, a website's design and layout in order to pass themselves off as a genuine (targeted) website. A malicious website is crafted which looks and feels like the original site, convincing unsuspecting users that they are giving personal information to a trusted organization.

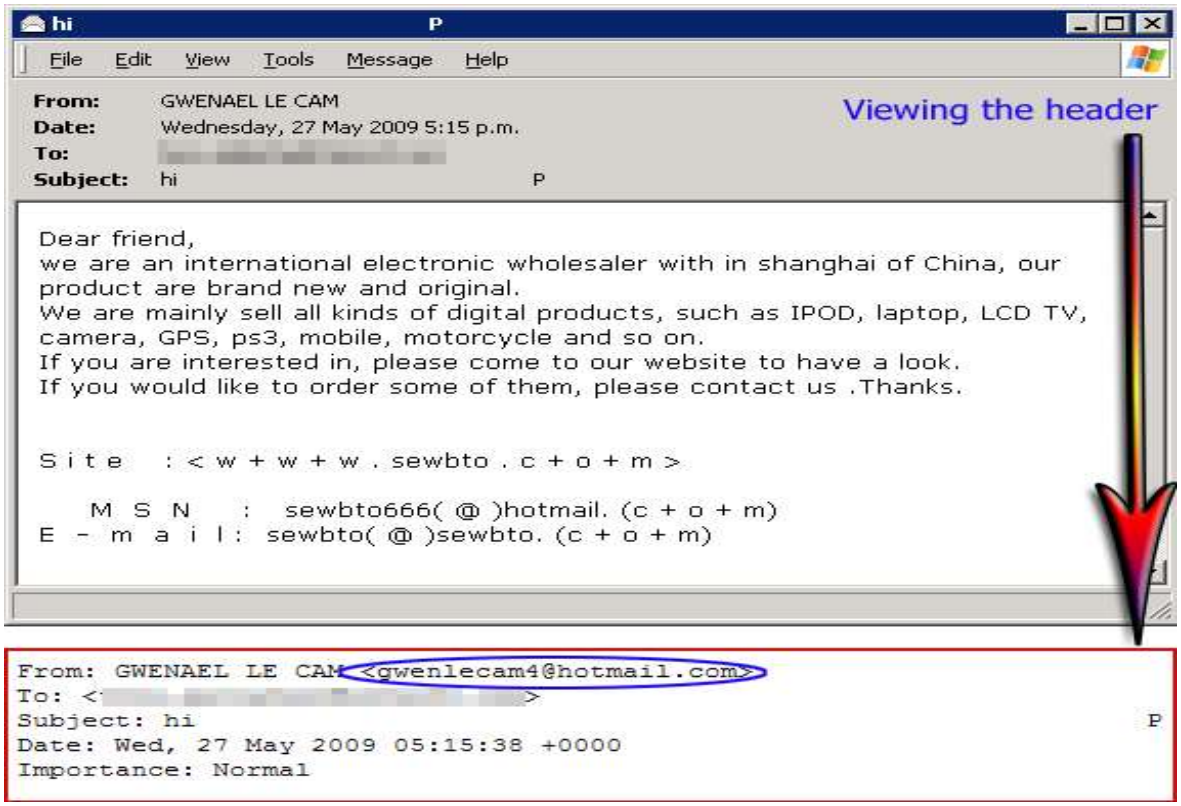
Users are frequently drawn to the sites by forged emails designed to look like legitimate correspondence and may even copy the body from real email, but when the user clicks a link to visit the website, they will be directed to the malicious site instead. The more convincing a phishing attack appears - or rather, the more genuine a malicious website looks - the more success the attack will have in extracting personal information. Some phishing attacks go so far as to create faux websites for which there is no legitimate counterpart; e.g. a page prompting users for personal information the organization wouldn't have otherwise asked for. According to Anti-Phishing Working Group (APWG), phishing activities have been increasing and most phishing websites are hosted in the US. In 2012, an average of over 25,000 unique phishing email reports were reported to the APWG. Plus, the number of unique phishing sites detected exceeded 45,000 per month [2].

2. PHISHING TECHNIQUES

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

2.1 Email Phishing

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



This scams usually introduces a website based in China selling cheap and branded electronics. If you weren't already suspicious from reading the email, you should be after viewing the website. It reeks of a scam, especially because of the payment method options when buying goods from them. The websites prefer payment through Western Union, Bank Transfer or MoneyGram. These types of payment methods are not recommended especially when dealing with people you don't know and trust [4].

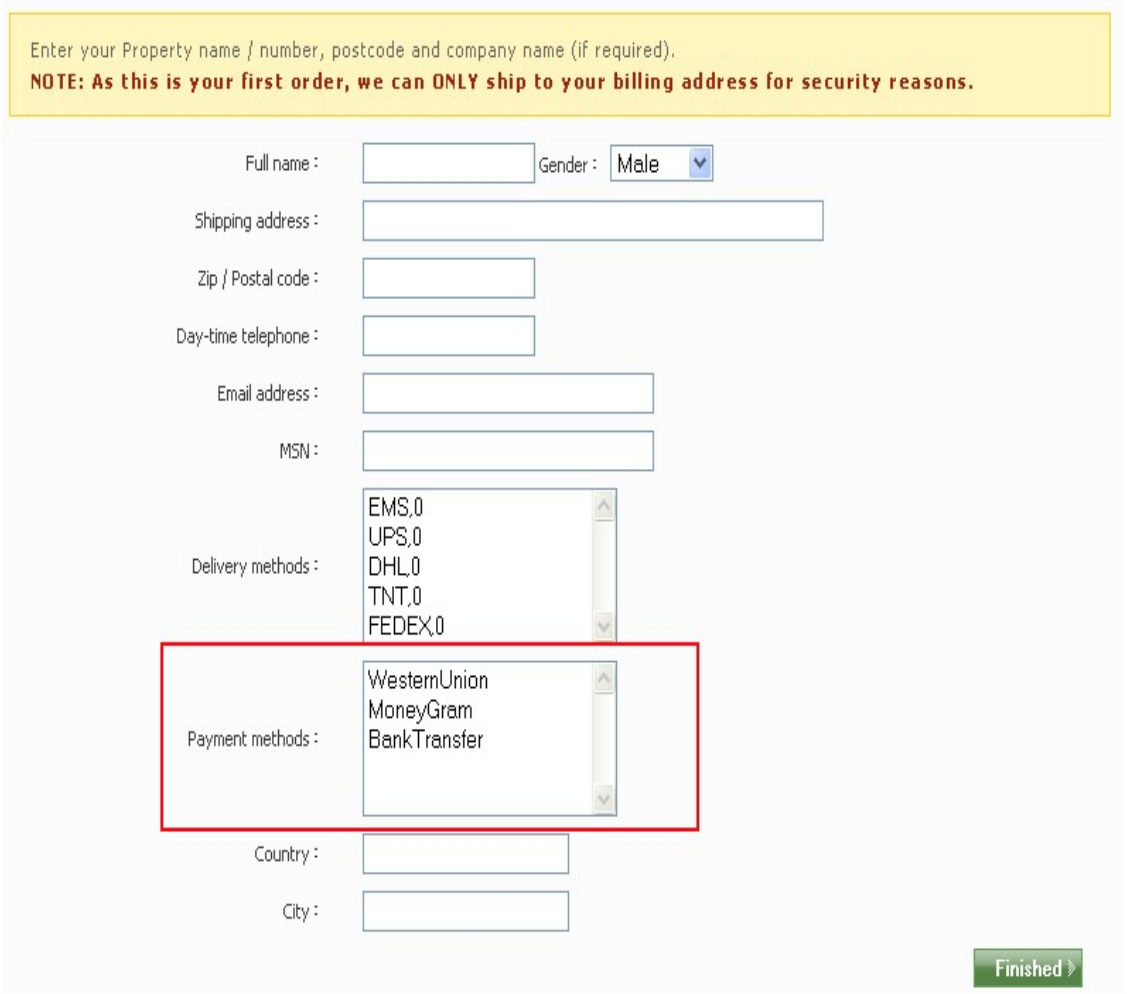


Fig 1: Sample Phishing Scam Order Form

Another suspicious thing is that, if this website was legitimate they would not use free email services like Hotmail to adverstise their wares. They could have at least used an email address using their own domain. Meanwhile, we noticed recently that Hotmail had actually moved to stop these spammers from abusing their free email service. A "Verify your Account" feature, which involve CAPTCHA verification was added to help prevent botnets from automatically sending spam. That's a welcome step. But in this case, it seems the spammers have found a way around it. Perhaps accounts are being manually verified prior to being used as spam conduits [4].

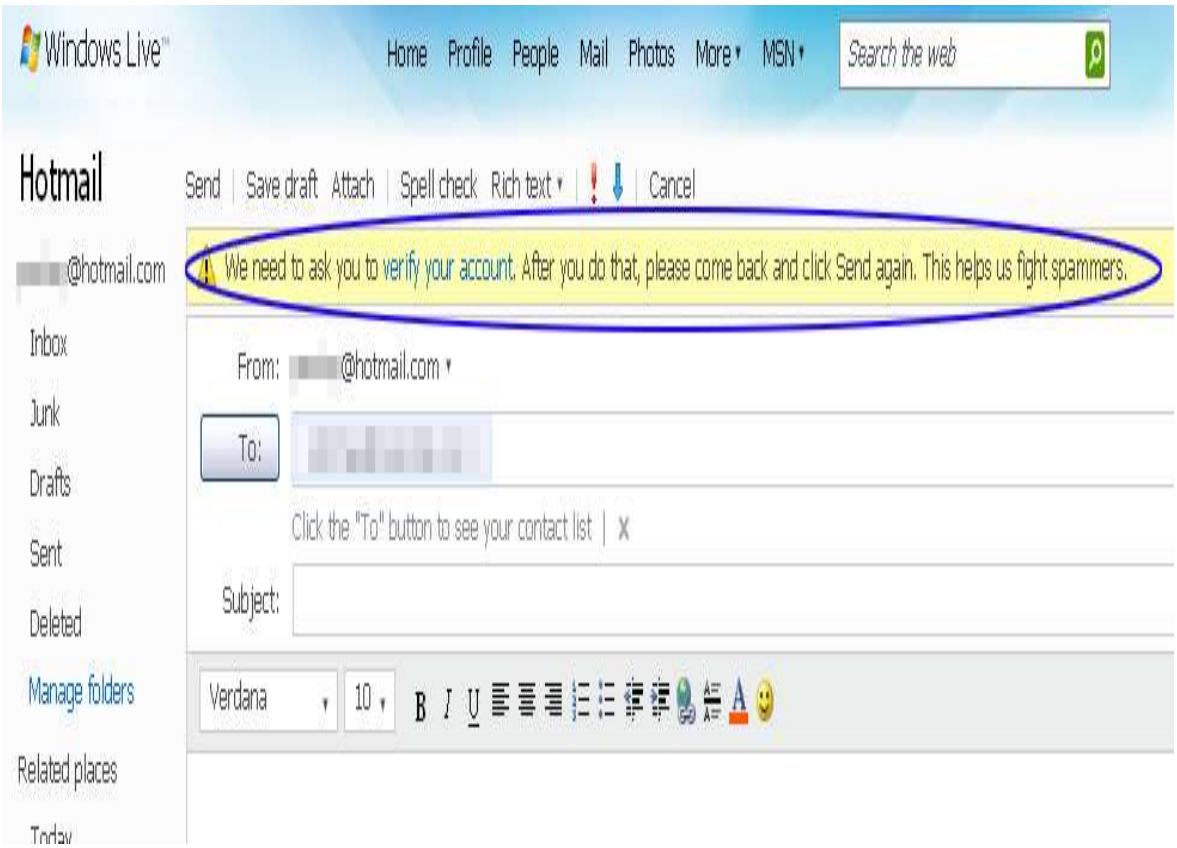


Fig 2: Sample Phishing Scam : Verification

2.2 Fruit Sucker

When another attacker breaks into a hacked, vulnerable website with an existing phishing page and changes the email address. Often since the attacker can see where the data is being emailed to he/she will keep the original email addresses intact and merely add his/her own email address in the BCC field. This is a very easy way for an attacker to make extra money. All passwords and account numbers keyed in reach his inbox directly without tipping off the original phishers. If the phishers are rookies and lack automated money transferring scripts, are too lazy to keep a watchful eye on their victims or are situated in a different time zone, then these advantages can help the fruit sucker withdraw a large amount of data (or other assets) from the compromised accounts before they do [6].

2.3 Spear Sucker

An attack against the original crackers. For example, a good guy who breaks into the phishing websites and changes the email address to the NEDBANK's CSO's or CEO's email address. After this he contacts the bank to make them aware of the security breach.

2.4 Haxtortionist

When an attacker patches the system, pulls down the phishing page and emails the attackers threatening them that he/she will report the crime and inform NEDBANK of their malicious activity. Reporting such abuse to email servers hosted by Google, Yahoo and similarly large companies in the United States is easy. In this way the attacker may extort a small share of money from the original crackers in return for keeping silent.

2.5 Robin-HAT

Here the attacker, after collecting a lot of passwords, changes the recipient's email address for the purpose of redistributing wealth. He/She withdraws money from the accounts and donates a significant portion to charity. Such individuals cannot be called grey hats because they are criminals robbing from other criminals. They are Robin-HATS, those who steal from rich victims and their attackers and redistribute the wealth to the poor and needy.

Another version on this above type of attack: the Robin-HATs uniformly redistributed the assets from the richer compromised accounts to the compromised accounts which had lower funds; especially if particular attention was paid to those accounts with low balances for a prolonged period of time.

2.6 Malware-based Phishing

Malware-based phishing involves running malicious software on the user's machine. The malware can be introduced as an email attachment or as a downloadable file exploiting security vulnerabilities. This is a particular threat for small and medium businesses (SMBs) who fails to update their software applications.

2.7 Session Hijacking Phishing

Session Hijacking is a kind of phishing attack where user's activities are monitored clearly until they log into a target account like the bank account and establish their credentials. At that point, the malicious software takes control and can undertake unauthorized actions, such as transferring funds, without the knowledge of the user.

2.8 Hosts File Poisoning Phishing

When a user types a URL of a website it is first translated into an IP address before it's transmitted over the Internet. The majority of user's PCs running a Microsoft Windows operating system first look up these "host names" in their "hosts" file before undertaking a Domain Name System (DNS) lookup. Phishers steal information by "poisoning" the hosts file. They transmit a bogus address, taking the user unwittingly to a fake "look alike" website.

2.9 System Reconfiguration Attacks

This is a kind of phishing attack where the settings on a user's PC are modified with bad intentions. For example: URLs in a favorites file might be modified to direct users to bogus websites that look alike. For example: a financial institution's website URL may be changed from "bankofxyz.com" to "bancofxyz.com".

3. MITIGATING PHISHING

The following information applies to functions available in browsers such as Opera, Internet Explorer, Chrome and Microsoft Firefox. Opera relies on blacklists from Netcraft and calls the feature a 'Fraud and Malware Protection [].

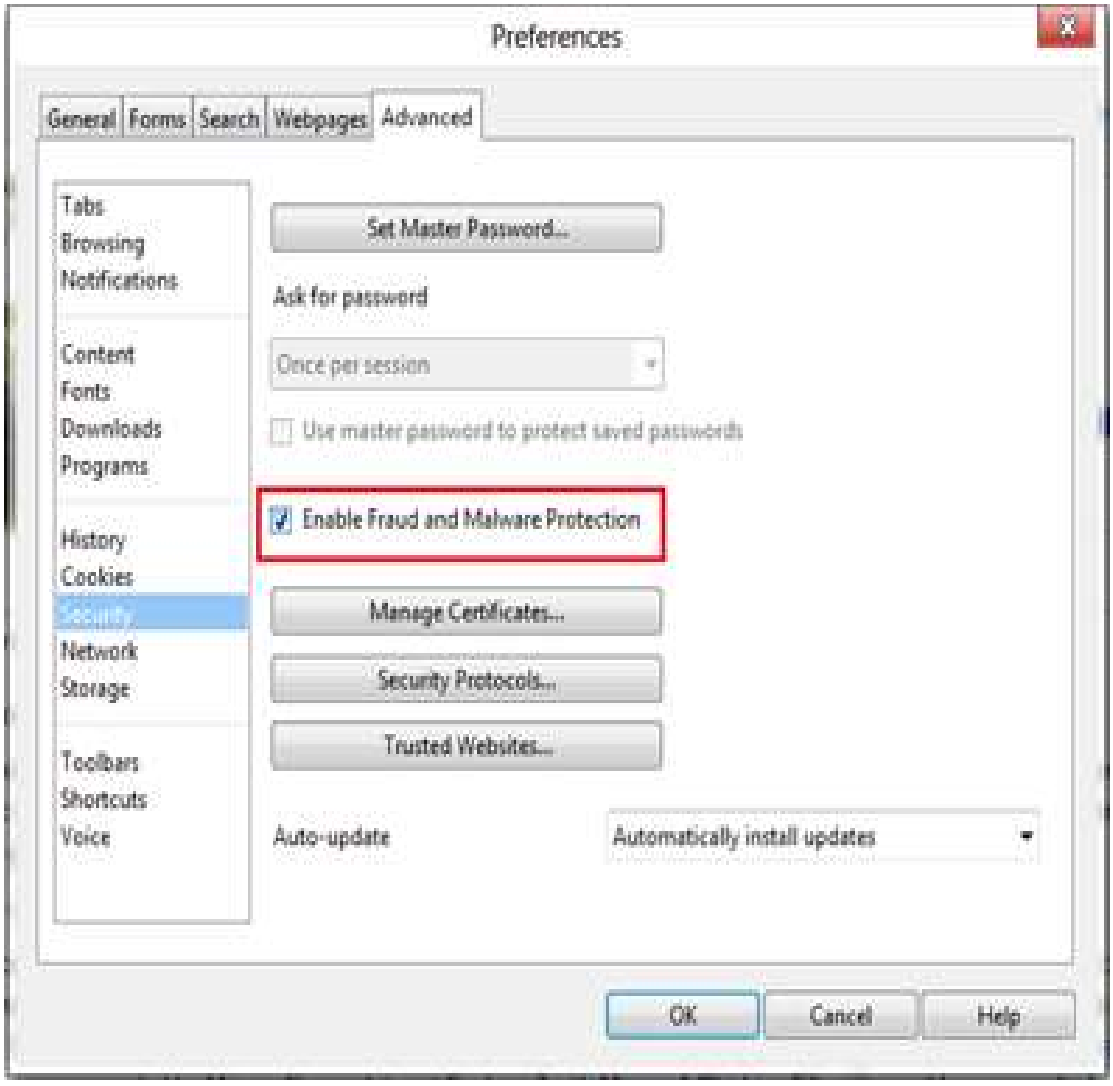


Fig. 3: Fraud and Malware Protection

Every URL you visit first goes to sitecheck2.opera.com (one of the noted IP is 91.203.99.45).
Microsoft Internet Explorer calls its feature to detect and report malicious websites a 'SmartScreen Filter.'

Fig. 4: Fraud and Malware Protection Window

It can be enabled as shown in the screenshot above or go to Tools / Internet Options/ <Navigate to the 'Security level for this zone' area> / Click on Custom level... / Miscellaneous/ Use SmartScreen Filter / Enabled.

Similar checks are done by Microsoft Internet Explorer, Chrome and Firefox.

Alternatively you can use OpenDNS as your DNS on your Ethernet and wireless cards IP configuration.

Although from personal observations, using OpenDNS takes you to a search engine (possibly powered by Google) on every website which fails to get resolved – and it might miss resolving a website hosting a phishing page.

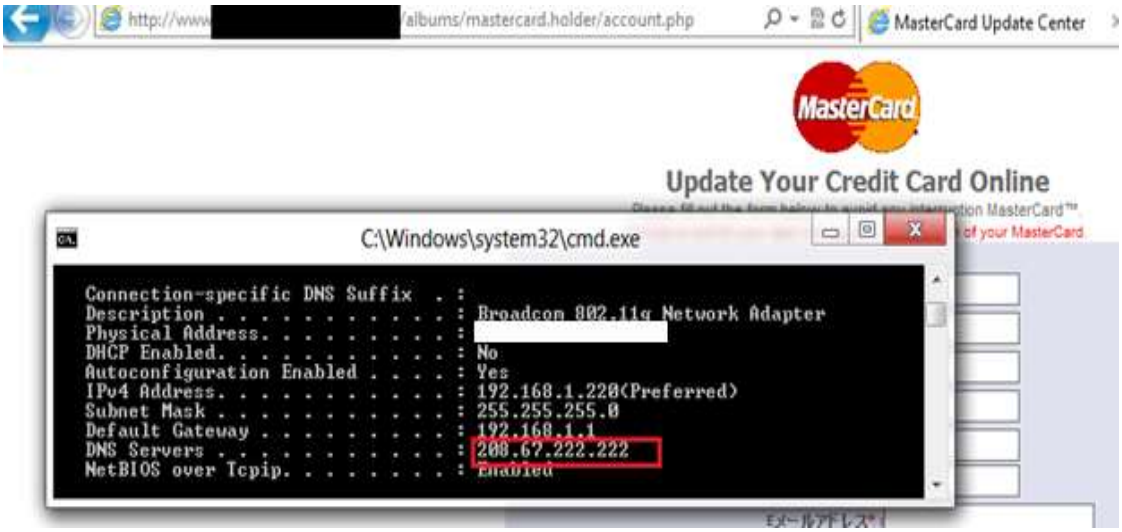


Fig. 5: Fraud and Malware Protection Framework Using OpenDNS

Still it is quite good at maintaining uncorrupted, un-poisoned DNS records. It's reliable when you suspect your ISP of injecting iframes, redirecting you and tracking your visits.

OpenDNS can be set by filing the DNS as 208.67.222.222 and 208.67.220.220 (as an alternative or vice-versa)

Such features greatly reduce the chances of a person falling prey to phishing websites if it has been reported. On an average it takes no more than 8 hours of hosting a phishing page before somebody reports it. This is a very long gap when you consider that in Asia banks are provided phishing alerts by third-parties who sign an SLA stating that they have to inform the bank within 5 minutes of a phishing page popping up on the Internet. The third-party will report the page to the banks and maybe even inform PhishTank, Netcraft, Haute Security, etc.

a. Pay attention to Grammar & Spelling. Many scammers are not native English speakers and this can be very apparent in their messages. Official businesses, on the other hand, usually take special care to use correct grammar and spelling.

b. If you can determine a message is sent from a legitimate organization but you don't want to receive additional messages, you can often use an 'Unsubscribe' from a link at the bottom of the message. However you should not 'Unsubscribe' from scam messages. Many scam messages include this to make them appear more legitimate and use this information to identify 'active' email accounts or possibly obtain sensitive information from users.

c. As an act of retaliation, some users will attempt to respond in anger or string spammers along to waste their time. However, these actions could provoke spammers and attackers into attempting to send more advanced, targeted messages to the user or find other ways to outright attack the user. The best course of action when dealing with spam is to delete and ignore the messages entirely.

4. CONCLUDING REMARKS

Phishing will always exist, because there will always be ways to trick people. The phenomenon of phishing is growing and the number of variations of techniques implemented demonstrates the high interest in these types of attacks by cybercrime. It's easy to look down upon the victims as being stupid, but often the people who fall for the tricks simply lack proper education about computers. The phenomena must be carefully studied. Fundamental is training people in the secure use of computer tools, the cyber threat that is looming, and how the user can recognize threats in order to avoid serious problems.

REFERENCES

[1] Phishing and Pharming: A Guide to understanding and mitigating the risks. http://www.cpni.gov.uk/documents/publications/2010/2010019phishing_pharming_guide.pdf?epslanguage=en-gb

[2] Phishing Attacks and How To Prevent From Being Hooked. http://www.hongkiat.com/blog/phishing-reports-prevention/

[3] A Novel Anti-Phishing Framework Based on Honeypots: In Proceedings of 4th Annual APWG eCrime Researchers Summit 2009 (APWG eCrime/eCRS 2009, Tacoma, WA, USA, October 20 & 21, 2009), IEEE. http://www.hooklee.com/default.asp?t=Honeypots4AntiPhishing

[4] A Little Spam with Your Bagle? http://labs.m86security.com/2009/06/page/2/

[5] Phishing: A Very Dangerous Cyber Threat. http://resources.infosecinstitute.com/phishing-dangerous-cyber-threat/

[6] Attacking the Phishers: An Autopsy on Compromised Phishing Websites http://resources.infosecinstitute.com/attacking-the-phishers/

[7] Phishing: http://labs.m86security.com/tag/phishing/

[8] What Exactly Is Phishing & What Techniques Are Scammers Using. http://www.makeuseof.com/tag/phishing-techniques-scammers/

[9] Security: Types of Phishing Scams & How to Recognize Them http://grok.lsu.edu/article.aspx?articleid=16680

[11] What are the Different Types of Phishing Attacks? http://www.innovateus.net/science/what-are-different-types-phishing-attacks

[12] Cut the Line on Phishing Scams http://www.visa.ca/en/personal/securewithvisa/phishing.jsp

[13] A Framework for Detection and Measurement of Phishing Attacks http://mmnet.iis.sinica.edu.tw/botnet/file/20100524/20100524_1.pdf