Phishing

Junxiao Shi, Sara Saleem

1 Introduction

Phishing is a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion [19]. The word "phishing" appeared around 1995, when Internet scammers were using email lures to "fish" for passwords and financial information from the sea of Internet users; "ph" is a common hacker replacement of "f", which comes from the original form of hacking, "phreaking" on telephone switches during 1960s [16]. Early phishers copied the code from the AOL website and crafted pages that looked like they were a part of AOL, and sent spoofed emails or instant messages with a link to this fake web page, asking potential victims to reveal their passwords [4].

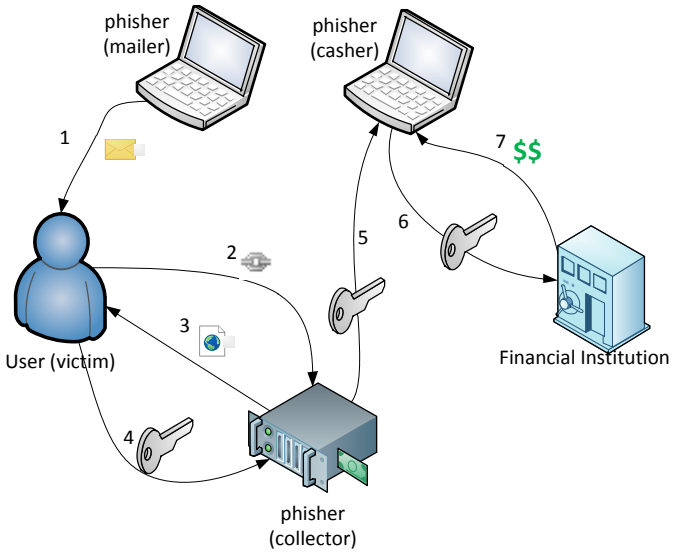

Figure 1: Phishing information flow

A complete phishing attack involves three roles of phishers. Firstly, *mailers* send out a large number of fraudulent emails (usually through botnets), which direct users to fraudulent websites. Secondly, *collectors* set up fraudulent websites (usually hosted on compromised machines), which actively prompt users to provide confidential information. Finally, *cashers* use the confidential information to achieve a pay-out. Monetary exchanges often occur between those phishers. The information flow is shown in Figure 1.

Before delving further into phishing it's important to clarify what is not phishing. Nigerian 419 scam (sending emails to trick recipients into giving money to the scammer) and Internet auction

fraud (non-delivery, misrepresentation, fee stacking, or selling stolen goods) are not considered phishing since they don't involve obtaining users' credentials [20].

The latest statistics reveal that banks and financial institutions along with the social media and gaming sites continue to be the main focus of phishers. Some loyalty programs are also becoming popular among phishers because with them phishers can not only breech the financial information of victim but also use existing reward points as currency. U.S. remains the largest host of phishing, accounting for 43% of phishing sites reported in January 2012. Next was Germany at 6%, followed by Australia, Spain, Brazil, Canada, the U.K., France, Netherlands, and Russia [29]. A study of demographic factors suggests that women are more susceptible to phishing than men and users between the ages of 18 and 25 are more susceptible to phishing than other age groups [30]. Phishing attacks that initially target general consumers are now evolving to include high-profile targets, aiming to steal intellectual property, corporate secrets, and sensitive information concerning national security.

2 Types of Phishing

Phishing has spread beyond email to include VOIP, SMS, instant messaging, social networking sites, and even multiplayer games. Below are some major categories of phishing.

2.1 Clone Phishing

In this type phisher creates a cloned email. He does this by getting information such as content and recipient addresses from a legitimate email which was delivered previously, then he sends the same email with links replaced by malicious ones. He also employs address spoofing so that the email appears to be from the original sender. The email can claim to be a re-send of the original or an updated version as a trapping strategy [31].

2.2 Spear Phishing

Spear phishing targets at a specific group. So instead of casting out thousands of emails randomly, spear phishers target selected groups of people with something in common, for example people from the same organization [28].

Spear phishing is also being used against high-level targets, in a type of attack called "whaling". For example, in 2008, several CEOs in the U.S. were sent a fake subpoena along with an attachment that would install malware when viewed [24]. Victims of spear phishing attacks in late 2010 and early 2011 include the Australian Prime Minister's office, the Canadian government, the Epsilon mailing list service, HBGary Federal, and Oak Ridge National Laboratory [18].

2.3 Phone Phishing

This type of phishing refers to messages that claim to be from a bank asking users to dial a phone number regarding problems with their bank accounts. Traditional phone equipment has dedicated lines, so Voice over IP, being easy to manipulate, becomes a good choice for the phisher. Once the phone number, owned by the phisher and provided by a VoIP service, is dialed, voice prompts tell the caller to enter her account numbers and PIN. Caller ID spoofing, which is not prohibited by law, can be used along with this so that the call appears to be from a trusted source [1].

3 Phishing Techniques and Countermeasures

Various techniques are developed to conduct phishing attacks and make them less suspicious. Email spoofing is used to make fraudulent emails appear to be from legitimate senders, so that recipients are more likely to believe in the message and take actions according to its instructions. Web spoofing makes forged websites look similar to legitimate ones, so that users would enter confidential information into it. Pharming attracts traffic to those forged websites. Malware are installed into victims' computers to collect information directly or aid other techniques. PDF documents, which supports scripting and fillable forms, are also used for phishing.

3.1 Email Spoofing

A spoofed email is one that claims to be originating from one source when it was actually sent from another [19]. Email spoofing is a common phishing technique in which a phisher sends spoofed emails, with the sender address and other parts of the email header altered, in order to deceive recipients.

Spoofed emails usually appear to be from a website or financial institution that the recipient may have business with, so that an unsuspecting recipient would probably take actions as instructed by the email contents, such as:

- reply the email with their credit card number
- click on the link labelled as "view my statement", and enter the password when the (forged) website prompts for it
- open an attached PDF form, and enter confidential information into the form (Section 3.5)

3.1.1 Sending a spoofed email

On a sendmail-enabled UNIX system, one line of command is all you need to send a spoofed email that appears to be from Twitter:

```
cat body.htm | mail -a 'From: Twitter <support@twitter.com>' -a '
    Content-Type: text/html' -s 'Reset your Twitter password'
    victim@example.net
```

The file body.htm contains the mail contents in HTML format. The result is shown in Figure 2.

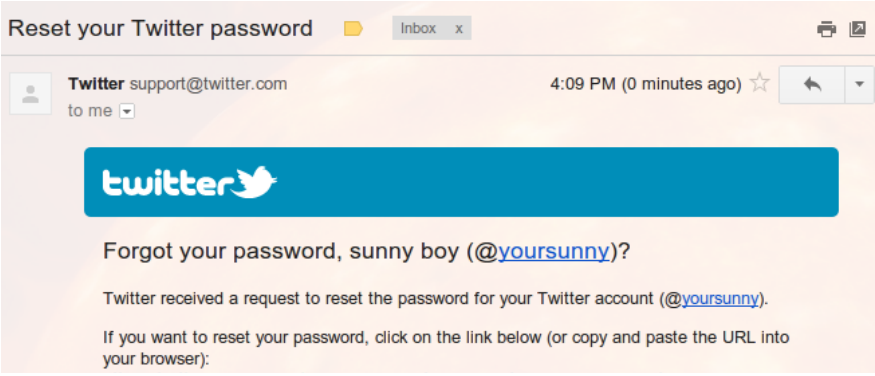

Figure 2: Fake Twitter password reset email received in Gmail

3.1.2 Why it's possible

Simple Mail Transfer Protocol [21] is the Internet standard protocol used for electronic mails. Its objective is to transfer mail reliably and efficiently, but core SMTP doesn't provide any authentication. An important feature of SMTP is its capability to transport mail across multiple networks, referred to as "SMTP mail relaying". Basically, receiving and relaying SMTP servers need to trust the upstream server; so it is feasible for a malicious user to construct spoofed messages, and talk with receiving or relaying SMTP servers directly to deliver such a message.

As RFC 5321 [21] suggests, SMTP mail inherently cannot be authenticated at the transport level; real mail security lies only in end-to-end methods involving the message bodies, such as Pretty Good Privacy (PGP) and Multipurpose Internet Mail Extensions (S/MIME). However, there is a high cost to deploy those digital signature based countermeasures, because users are reluctant to install an additional piece of software, and they don't have enough knowledge on how to manage the trust.

3.1.3 SPF

Sender Policy Framework (SPF) is an open standard specifying a technical method to prevent sender address forgery [25]. Since most SMTP servers are mutually-TCP-addressible hosts on the public Internet, receiving and relaying SMTP servers are able to see the IP address of the sending host. SPFv1 protects the *envelope sender address*, the `HELO` domain and the `MAIL FROM` address, by verifying sender IP addresses: SPFv1 allows the owner of a domain to specify a list of IP addresses that are allowed to send emails from their domain, and publish this information in the domain's DNS zone; a receiving server may query DNS to check whether the message comes from one of those whitelisted addresses.

For example, cs.arizona.edu publishes the following SPF record:

```
v=spf1 a:gandalf.email.arizona.edu a:frodo.email.arizona.edu a:pacer.emai
l.arizona.edu a:gremlin.email.arizona.edu a:optima.cs.arizona.edu ~all
```

This SPF record lists 5 hostnames, and these hosts are allowed to send emails on behalf of @cs.arizona.edu; "~all" disallows any other hosts to send emails from this domain.

3.1.4 DKIM

DomainKeys Identified Mail (DKIM) allows an organization to take responsibility for transmitting a message in a way that can be verified by a recipient. The author, the originating sending site, an intermediary, or one of their agents can attach digital signatures onto a message [17]. The message headers and body, including the originator address (the `From` header field), are signed. The `DKIM-Signature` header field includes the signature, the signing domain, and information about how to retrieve the public key.

A DKIM signature generated by Gmail looks like:

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
  d=gmail.com; s=gamma;
  h=domainkey-signature:mime-version:received:received:in-reply-to
   :references:date:message-id:subject:from:to:content-type;
  bh=rdk+ZKX52H558uYXf2No2gW+cp8RKaZBZwyOM+LufnE=;
  b=dw0s8c2uuBIqY8msh1266XyGlTDxYGwIBmuVPpkMEUGh2mrhWaUwSWYUnOKHSh
   vlwVBTiLGRQ8t8KYk1XdMveBnE3iaXlOGiGKlQLqIQjyd+sxbc8OSGHxcO05BpO
```

```
3Egb/pf+i8m9iktEjN4PPhLKsyiniNO8vy8LqC33zjyiVw=
```

The signing domain publishes public keys as TXT records in their DNS zone. To verify this signature, a receiving server may query DNS name gamma._domainkey.gmail.com (constructed from tags "s" and "d" of the signature) and get a TXT record such as:

```
k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDIhyR3oItOy22ZOaBrIVe9m/iM
E3RqOJeasANSpg2YTHTYV+Xtp4xwf5gTjCmHQEMOs0qYu0FYiNQPQogJ2t0Mfx9zNu06rfRBD
jiIU9tpx2T+NGlWZ8qhbiLo5By8apJavLyqTLavyPSrvsx0B3YzC63T4Age2CDqZYA+OwSMWQ
IDAQAB
```

Then the signature can be verified using RSA and SHA-256 algorithms, as specified in tag "a".

3.1.5 Other detection methods

Microsoft's SenderID validates the sending server's IP addresses against a TXT record published in the originator address's DNS zone [27, 26].

Heuristic-based detection techniques are proposed to identify phishing emails. For example, a simple heuristic is the observation that emails generated by the same toolkit show a high degree of similarity [33]. Once the heuristic identifies a kind of phishing emails, it can be entered into a blacklist, and further emails will be blocked.

3.2 Web Spoofing

A phisher could forge a website that looks similar to a legitimate website, so that victims may think this is the genuine website and enter their passwords and personal information, which is collected by the phisher.

Modern web browsers have certain built-in security indicators that can protect users from phishing scams, including domain name highlighting and https indicators. However, they are often neglected by careless users.

3.2.1 How web spoofing is done?

Creating a forged website It's trivial to clone the look of a website by copying the front-end code; a little bit of web programming is necessary to redirect user's input into a file or database, then show a "website under maintenance" notice.

Proxy software such as `squid` [8] or `Fiddler2` [22] could be extended to create a fully functional clone. Users can successfully sign in and use all the services provided by the original website, while all the inputs are collected by the server, and all the pages may be modified by the server.

Attracting traffic to forged website Once a forged website is online, the phisher must make potential victims visit it. There are a few ways to do this:

- Send spoofed emails (section 3.1) with a link to the forged website.
- Register a domain that is a common typo of a popular website. For example, register `paypel.com` and create a forged `paypal.com`.
- Register the same domain name in a different TLD. Sometimes people will type in their country-specific TLD and expect to get a "localized" version of the website. For example, register `gmail.com.cn` and create a simplified-Chinese forged version of `gmail.com`.

- Do search engine optimization.
- Use pharming (section 3.3).

3.2.2 Browser security indicator: Domain name highlighting

Figure 3: Different highlighted domain names show that these website are unrelated

Phishers tend to use misleading addresses, such as `http://www.paypal.com.cgi-bin.webcr.example.com/`, to deceive users. With domain name highlighting, users can easily interpret the address and identify the current website at a glance (Figure 3). [2]

With domain name highlighting, most web spoofing attacks can be identified, unless the phisher is using pharming.

3.2.3 Browser security indicator: HTTPS padlock

(a) http, no padlock (b) padlock on https

Figure 4: A padlock icon appears in address bar when visiting an https website

HTTPS, the combination of Hypertext Transfer Protocol and Transport Layer Security, provides encryption and identification through public key infrastructure. Modern web browsers display a padlock icon when visiting an https website (Figure 4).

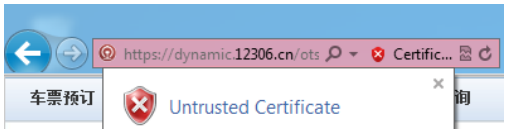

Figure 5: The address bar turns red on invalid certificate

Figure 6: The padlock icon disappears on mixed content

Web browsers verify the certificate presented by the web browser. The certificate is considered invalid if any of the following applies: the certificate is expired; the certificate is not signed by a root CA trusted by the local computer; the certificate is revoked by the CA; the website host name does not match the subject names in the certificate. In this case, there is likely a Man-In-The-Middle attack, so the browser will display a prominent warning (usually a full page), and the address bar would turn red if the user choose to continue onto the website (Figure 5).

Sometimes an https webpage may contain files from http scheme. Every piece of code should be trusted, before a webpage can be trusted. Thus, the padlock icon would disappear (Figure 6).

3.2.4 Effectiveness of browser security indicators and HTTPS

Browser security indicators are not as effective as one might think. A survey [13] reports that 23% of participants used only the content of a webpage to determine legitimacy; an identical-looking clone

under any domain name without https is enough to deceive them. Many users cannot distinguish between a padlock icon in the browser chrome and a padlock icon as the favicon or in the page contents.

Relying on HTTPS is also not sufficient. Malware can install the public key of a phisher's CA to local computer's trusted root CA list, so that certificate signed by this CA would be trusted. When the phishing website is using a similar-looking domain that is registered by the phisher, a real certificate can be requested after domain ownership verification. CAs could be hacked to issue fraudulent certificates [10]. Moreover, if a government is involved in phishing, it can order a CA under its control to issue a certificate for the phishing server.

3.2.5 Other countermeasures

Dynamic Security Skins [12] seems to be a good method. The idea is that the website server generates a unique abstract image for each user, and the web browser also independently computes the same image. The algorithm ensures that a phisher cannot predict this image. The user just needs to compare these two images; if they are identical, the server is legitimate.

3.3 Pharming

Pharming is a type of attack intended to redirect traffic to a fake Internet host. There are different methods for pharming attacks, among which DNS cache poisoning is the most common.

3.3.1 The DNS, and DNS cache poisoning

Domain Name System (DNS) is a critical piece of Internet infrastructure. Designed as a distributed system, DNS publishes a hierarchical database by a hierachy of name servers. To improve performance, clients contact local DNS resolvers maintained by local ISPs, which can cache records from name servers. Clients, resolvers, and name servers talk with each other on UDP port 53. [35]

DNS is critical to Internet security. As shown in Section 3.1, SPF, DKIM, and SenderID all rely on DNS; if DNS is compromised, spoofed emails can get through these signature-based countermeasures. Web spoofing can also be conducted by making DNS respond with the address of phisher's server.

DNS cache poisoning attempts to feed the cache of local DNS resolvers with incorrect records. This is possible because: DNS runs over UDP, and it's easy to spoof the source address of a UDP packet; the DNS packet header contains a 16-bit query ID field, which is relatively short so a birthday attack is feasible.

Domain Name System Security Extension (DNSSEC) [14] is an extension of DNS that provides three distinct services: key distribution, data origin authentication, and transaction and request authentication. Every DNS record can be authenticated via a chain of trust. Cache poisoning is no longer possible, because the phisher cannot produce a correct signature without knowing the private key of the domain. However, DNSSEC is not widely deployed yet.

Google Public DNS, the largest public DNS resolver in the world, mitigates cache poisoning attacks by adding entropy to queries: [7]

- use a random source UDP port
- randomly choose a name server among configured name servers of a zone
- randomize case in the query name. eg. `wWw.eXaMpLe.CoM` and `WwW.ExamPLe.COm` are equivalent

- prepend a nonce label to the query name, if the response is known to be a referral. eg. sending `entriih-f10r3.www.google.com` in a query to root servers

These randomness makes it much harder to construct a matching response than using the 16-bit query ID alone. Thus, cache poisoning is no longer feasible.

3.3.2 Domain hijacking

A more advanced pharming attack is domain hijacking. In domain hijacking, the DNS delegation record at the domain registrar is changed to a name server controller by a hacker, so that all traffic can be redirected globally.

Baidu, the largest search engine in China, was hacked by Iranian Cyber Army in January 2010. [15]

1. The hacker chatted with technical support of Register.com, the domain registrar of baidu.com, to change the email address on file. The change was approved without careful verification.
2. Account password was reset with the new email address.
3. Delegation record was changed to a name server controlled by the hacker.
4. Millions of users were redirected to hacker's server for 4 hours.

A phisher could also use similar techniques to gain control over a domain.

3.3.3 Pharming in smaller scope

DNS cache poisoning and domain hijacking are effective in a large scope, so they would be quickly found and fixed. There are techniques for pharming in a smaller scope, such as the local computer or a home network, that can possibly remain unnoticed for a longer term.

The hosts file is a text file on local computer that contains hostname-to-IP mappings. This file is located at `/etc/hosts` in UNIX systems, or `%WINDIR%\system32\drivers\etc\HOSTS` in Windows systems. TCP/IP stack consults this file before querying DNS. This file could be written by malware for pharming.

ARP spoofing can manipulate traffic in local Ethernet, including redirecting traffic to phishing server. It can be implemented in malware.

In regions of world that Internet is restricted, some people offer solutions that claim to provide uncensored access to Internet. These solutions usually come as software, VPN, proxy server, or hardware home router; they could be either paid or free. A dishonest provider could offer such a solution with pharming built-in, and users looking for uncensored access would end up visiting forged websites without realizing this.

3.4 Malware

Malware is a piece of software developed either for the purpose of harming a computing device or for deriving benefits from it to the detriment of its user [19]. Malware can be used to collect confidential information directly, or aid other phishing techniques.

Client security products are able to detect and remove malware and other potentially unwanted programs, but phishers can make malware undetectable. Financial institutions and online game vendors distribute security programs to protect their customers.

3.4.1 Phishing with malware

Malware can be used to collect confidential information directly, and send them to phishers. Keystrokes, screenshots, clipboard contents, and program activities can be collected. Password input box, where letters are shown as asterisks, can be easily read with a program. Malware can also display a fake user interface to actively collect information. Collected information can be automatically sent to phishers by email, ftp server, or IRC channel.

Malware can also aid other phishing techniques. For web spoofing, it can install phisher's CA public key into local computer's trusted CA list. For pharming, it can change the hosts file or DNS settings, or even run ARP spoofing on local Ethernet. Malware can also enlist the computer into botnets, to send spoofed emails or act as a webserver of forged websites.

3.4.2 Detecting malware with client security products

Client security products are widely deployed. Microsoft Update also pushes "Malicious Software Removal Tool" monthly, which is a lightweight malware scanner.

However, they are not always effective. It's easy to modify a program so that it doesn't contain any known signature, to bypass signature-based detection. There are also techniques to bypass certain behavior-based detection.

3.4.3 Protection for online banking

Figure 7: online banking client from China Merchants Bank

Figure 8: USB token

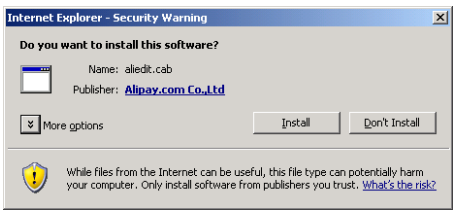

Figure 9: secure text input control from Alipay.com

Financial institutions, the most common targets of phishing, distribute security programs to protect their customers. They usually come in the form of client programs (Figure 7) or browser add-ons (Figure 9). These programs can protect customers in one or more ways:

- implement a secure text input control, usually by using a kernel-space driver, so that (most) keyloggers cannot intercept the keystrokes or read its contents
- encrypt confidential information in memory and in network
- block or remove known malware
- verify the certificate of the financial institution, to protect against Man-In-The-Middle attacks

- make use of hardware tokens or smart cards (Figure 8)

Some of these modes of protection are quite effective but not perfect:

- Like every other program, there may be vulnerabilities in those 'security' programs [23].
- Malware can hide the user interface of the security program, and display a fake user interface.

Hardware tokens are secure enough, if carefully designed. There is one case [34] that a swindler tricked an old man to run a Trojan horse, plug in his USB token, reveal his bank password, and turn off the computer monitor, and then the swindler transferred money out of the account; however that case is out of the scope of phishing.

3.5 Phishing through PDF Documents

Adobe's Portable Document Format is the most popular and trusted document description format. This makes PDF documents more susceptible to phishing threats, owing to their portability and interoperability on multiple platforms. In addition to being a powerful document format, PDF is a comprehensive programming language of its own dedicated to document creation and manipulation with strong execution features. Some critical functions of a PDF language could be misused by an attacker or a hacker to design a PDF document to his/her own advantage and extract the desired information from the victim, thereby creating a new worldwide threat. These potentially dangerous functions include `OpenAction` and `SubmitForm`.

Although Adobe has implemented some security mechanisms in Adobe Reader and Adobe Acrobat in order to alert the user in case of (potentially) malicious attempts, these alert measures are just message boxes, asking the user to allow or block an action. Unfortunately, such message boxes are often neglected by users, and it is possible to bypass these security mechanisms by modifying RdLang32.FRA and AcroRd32.dll files with malware. [11]

4 Additional Preventive Measures

Given the risk of phishing, what are the ways in which individuals and organizations can protect themselves? Though hard to implement but training the end-user is perhaps the best protection mechanism. Sensing the gravity of issue, more non-profit organizations and groups are joining hands to combat phishing scams. Legislation particularly needs attention in this matter to define phishing explicitly and elucidate phishing specific penalties

4.1 User Education

Phishing exploits human vulnerabilities such that technical solutions can only block some of the phishing web sites. It doesn't matter how many firewalls, encryption software, certificates, or two-factor authentication mechanisms an organization has if the person behind the keyboard falls for a phishing attack.

A study on effectiveness of several anti-phishing educational materials suggests that educational materials reduced users' tendency to enter information into phishing webpages by 40%; however, some of the educational materials also slightly decreased participants' tendency to click on legitimate links [30]. This leads to the belief that it is of paramount importance to find a new and efficient way of educating a large proportion of the population[32]. The challenge lies in getting the user's attention to these security tips and advises.

There are few questions that arise: Should we implement all these protection mechanisms which complicates the user interface? Should we provide better user experience at the cost of reduced security or improve security at the cost of user inconvenience? Several recent surveys indicate that lack of security is leading to loss of customer confidence in Internet commerce. That means users want appropriate security controls in place even if it means carrying a password token or getting their passwords on SMS. Today phishing is recognized by users as a real and potentially damaging threat. If appropriate anti-phishing controls are not put in place, chances are high that customers might switch to a more secure party to do business.

4.2 Anti-Phishing Groups

PhishTank, launched in October 2006, is a collaborative clearing house for data and information about phishing on the Internet. PhishTank employs a sophisticated voting system that requires the community to vote "phish" or "not phish", reducing the possibility of false positives and improving the overall breadth and coverage of the phishing data. It also provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge. PhishTank is backed by OpenDNS, a public DNS resolver; OpenDNS utilizes PhishTank data to prevent phishing attacks for their users.

Formed in 2003, the Anti-Phishing Working Group (APWG) is an international consortium that brings together businesses affected by phishing attacks, security products and services companies, law enforcement agencies, government agencies, trade association, regional international treaty organizations, and communications companies [3].

FraudWatch International, a privately owned Internet security company established in 2003, provides a variety of anti-phishing products and services to protect financial service, e-commerce, and Internet hosting companies from phishing.

4.3 Legal Aspects

Currently little legislation related to phishing exists; this appears to be due to a lack of awareness at the governmental level. In order for technical and educational solutions to be successful, government support is required.

The UK Fraud Act of 2005 covers fraud by false representation, however this does not specifically mention phishing; suggesting that not only the end users but also the governments are unaware of the dangers of phishing [32].

In 2005 a bill named The Anti-Phishing Act of 2005, "A bill to criminalize Internet scams involving fraudulently obtaining personal information, commonly known as phishing", was presented in United States Senate to combat phishing and pharming. The bill proposed a five-year prison sentence and/or fine for individuals who commit identity theft using falsified corporate websites or e-mails. Thus it allows law enforcement officials to fight phishing scams, by creating an opportunity to prosecute before the actual fraud takes place [6].

The Anti-Phishing Act couldn't become a law at federal level, but there are a few states including California, New Mexico, Arizona, and Texas which have strict anti-phishing laws in place [9].

Besides this there is still much work to be done on international basis. Most phishing scams operate overseas and it is exceedingly difficult and time consuming to prosecute an individual residing in a foreign country [5].

References

[1] Identity thieves take advantage of voip. http://www.icbtollfree.com/article_free.cfm?articleId=5926.

[2] Internet explorer 8 features - safer: domain highlighting. http://windows.microsoft.com/en-US/internet-explorer/products/ie-8/feat%ures/safer?tab=ie8dom.

[3] Opendns' phishtank.com and anti-phishing working group to share data. http://www.opendns.com/about/announcements/19/.

[4] Phishing - word spy. http://www.wordspy.com/words/phishing.asp.

[5] Phishing- consumer laws. http://consumerprotection.uslegal.com/phishing/.

[6] Proposed law aims to fight phishing. http://www.pcworld.com/article/119912/proposed_law_aims_to_fight_phishi%ng.html.

[7] Public dns security benefits. https://developers.google.com/speed/public-dns/docs/security.

[8] squid: Optimising web delivery. http://www.squid-cache.org/.

[9] Taking legal action against phishers. http://www.sis.pitt.edu/~nophish/expert/legal.html.

[10] Heather Adkins. An update on attempted man-in-the-middle attacked. http://googleonlinesecurity.blogspot.com/2011/08/update-on-attempted-ma%n-in-middle.html, Aug 2011.

[11] Gundeep Singh Bindra. Masquerading as a trustworthy entity through portable document file (pdf) format. In *Privacy, Security, Risk and Trust (PASSAT), 2011 IEEE Third International Conference on and 2011 IEEE Third International Confernece on Social Computing (SocialCom)*, pages 784 –789, Oct 2011.

[12] Rachna Dhamija and J. D. Tygar. The battle against phishing: Dynamic security skins. In *Proceedings of the 2005 symposium on Usable privacy and security*, SOUPS '05, pages 77–88, New York, NY, USA, 2005. ACM.

[13] Rachna Dhamija, J. D. Tygar, and Marti Hearst. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, CHI '06, pages 581–590, New York, NY, USA, 2006. ACM.

[14] D. Eastlake 3rd. Domain Name System Security Extensions. RFC 2535 (Proposed Standard), March 1999. Obsoleted by RFCs 4033, 4034, 4035, updated by RFCs 2931, 3007, 3008, 3090, 3226, 3445, 3597, 3655, 3658, 3755, 3757, 3845.

[15] Owen Fletcher and Robert McMillan. Baidu: Registrar 'incredibly' changed our e-mail for hacker. http://www.computerworld.com/s/article/9162118/Baidu_Registrar_incredib%ly_changed_our_e_mail_for_hacker, 2010.

[16] Anti Phishing Working Group. Origins of the word "phishing". http://www.antiphishing.org/word_phish.html.

[17] T. Hansen, D. Crocker, and P. Hallam-Baker. DomainKeys Identified Mail (DKIM) Service Overview. RFC 5585 (Informational), July 2009.

[18] Jason Hong. Why have there been so many security breaches recently? http://cacm.acm.org/blogs/blog-cacm/107800-why-have-there-been-so-many-%security-breaches-recently/fulltext.

[19] Markus Jakobsson and Steven Myers. *Phishing and countermeasures: understanding the increasing problem of electronic identity theft*. John Wiley & Sons, Inc., 2007.

[20] Lance James. *Phishing Exposed*. Rockland, MA : Syngress, 2005.

[21] J. Klensin. Simple Mail Transfer Protocol. RFC 5321 (Draft Standard), October 2008.

[22] Eric Lawrence. Fiddler web debugger - a free web debugging tool. http://www.fiddler2.com/fiddler2/.

[23] luoposhusheng. Plaintext disclosure vulnerability of alipay password security control. *Hacker Defense*, pages 6–8, Nov 2011.

[24] John Markoff. Larger prey are targets of phishing. http://www.nytimes.com/2008/04/16/technology/16whale.html.

[25] Julian Mehnle. Sender policy framework - introduction. http://www.openspf.org/Introduction.

[26] Julian Mehnle. Spf vs sender id. http://www.openspf.org/SPF_vs_Sender_ID.

[27] Microsoft. Sender id framework overview. http://www.microsoft.com/mscorp/safety/technologies/senderid/overview.m%spx, Sep 2004.

[28] Federal Bureau of Investigation. Spear phishers. http://www.fbi.gov/news/stories/2009/april/spearphishing_040109.

[29] PhishTank. Phishtank stats-jan 2012. http://www.phishtank.com/stats/2012/01/?y=2012&m=01.

[30] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, and Lorrie Cranorand Julie Downs1. Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. In *28th international conference on Human factors in computing systems*, Apr 2010.

[31] Wikipedia. Phishing — wikipedia, the free encyclopedia. http://en.wikipedia.org/w/index.php?title=Phishing&oldid=484977983, 2012. [Online; accessed 2-April-2012].

[32] C. Wilson and D. Argles. The fight against phishing: Technology, the end user and legislation. In *Information Society (i-Society), 2011 International Conference on*, pages 501 –504, Jun 2011.

[33] Guang Xiang, Bryan A. Pendleton, Jason Hong, and Carolyn P. Rose. A hierarchical adaptive probabilistic approach for zero hour phish detection. In *Proceedings of the ESORICS 15th European Symposium on Research in Computer Security*, pages 571–589, 2010.

[34] Yiru Xu. 67-year-old man swindled 700k from online banking account. http://finance.sina.com.cn/money/bank/guangjiao/20110326/16149598471.sh%tml.

[35] Beichuan Zhang. Domain name system (dns).