Volume 4, Issue 10, October 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Towards Mitigation of Phishing: The State of web Client Anti-phishing Technologies

Thomas Nagunwa
Department of Computer Science, Institute of Finance Management, Tanzania

Abstract - To adapt to the fast growing and evolving nature of phishing attacks, new web client based anti-phishing solutions are being adopted while old ones improved over the years. Recently introduced multifactor authentication methods are becoming popular in e-commercein mitigating credentials hacking and man-in-the-middle attacks. Extended validation SSL certificate was introduced to improve SSL certificate through implementation of strict business validation procedures. Browsers and anti-malware vendors have improved their anti-phishing features to cope with modern trends of attacks while new anti-phishing plugins are being developed to complement browser built-in anti-phishing capabilities. This paper reviews the current state of web client anti-phishing tools deployed in the web communities as well as the proposed solutions by security researchers. Learning these tools increases awareness to users, businesses and organizations on available anti-phishing techniques, their capabilities and ways to adoptthem. The paper observes thatmost of anti-phishing filters have high phishing detection rates of up to 99% and few false positives. However, most of the tools have their anti-phishing features disabled by default while provide passive warnings with options for users to ignore them.Each technology provides effective protection against particular phishing vectors only but can be vulnerable to other vectors. It is concluded that for effective phishing mitigation, several technologies should be deployed in combination to offer protection over a wide range of phishing vectors.

Keyword -security, phishing, user credentials, browser, URL, plugins, email

I. INTRODUCTION

Phishing is the useof different enticing skills including technology and social engineering to trick online users into giving up their online credentials and purporting them to steal money and secrets, control the host to launch massive attacks or make unauthorized online purchases [1]. Over the years, phishing activities leading to fraud have caused many economic and social damages to online communities. In 2012, for instance, global online consumers experienced a total loss of US $110 billion when 556 million consumers were victimized in more than 30 million hacking activities including phishing [2], [3]. Some business brands have lost reputations and confidence towards sections of their online markets leading to fall of businesses [4].Corporates and government agencies have lostintellectual properties and secrets to competitors and national enemies respectively.

To elude users and overcome technological and social anti-phishing strategies, phishers have been adopting diversified and evolving phishing vectors. Major phishing vectors deployed today are phishing spams, use of malware, vishing, pharming, SQL injection and cross site scripting[5]. Recently adopted but are becoming prominent phishing vectors are spear phishing, black hat search engine optimization (SEO), use of rogue SSL certificates, mobile phone phishing, social media and web 2.0 phishing as well as cloud computing phishing [5].

In response to the wide spread and evolving nature of phishing attacks, security community has developed and proposed adaptive web client technologies to help users from being phishing victims. This paper categorizes these solutions as

- User multifactor authentication: authentication methodsusing at least two credentials to authenticate the same user.
- Browser encryption technologies: web protocols that secure web page traffic between user and server while authenticate the two entities.
- Browser anti-phishing tools: built-in and plugins tools that detect and filter out phishing websites.
- Anti-malware software: software to detect, remove or isolate malicious programs in a host.
- Email filters: email applications built-in or plugins tools that detect, delete or isolate phishing email from user's inbox
- Anti-phishing training tools: tools that train users on ways to identify real world phishing URLs and emails.
- Proposed anti-phishing solutions: these are highly performing solutions that were researched by security experts but are yetavailable for massive use.

The study explores how these tools work while highlighting their performances, strengths and shortcomings. This will help users, especially those who are aware of phishing, to understand availability and varieties of tools in the market to select from depending on their protection needs. Users should be able to learn which features to enable to attain maximum protection as well as the need to deploy more than one solution for ultimate security. Businesses and

organizations should also learn tools to deploy to protect and train their customers and staff on best practices for phishing free web uses.

Next sections describe web client anti-phishing technologies.

II. USER MULTIFACTOR AUTHENTICATION

To limit abuse of onefactor authentication for phishing attacks, security researchers, experts and authorities such as USA's Federal Financial Institutions Examination Council (FFIEC) and Council of European Professional Informatics Societies (CEPIS) have recommended the use of multifactor authentication (MFA) methods to limit access to online financial institutionsespecially in the internet banking[6], [7], [8]. The methods deploy at least two credentials to authenticate the user. Credentials may include password, smart cardPIN, one-time password (OTP) token, image, secret key, user selected picture, biometric characteristics, and others [6],[7]. Each credential provides an independent security layer which represents what use know (e.g password), what user has (e.gsmart card) and what user is (e.g fingerprint)[9]. MFA deploys at least two of these layers. With MFA, when one security layer is compromised, the other layer(s) provide extra protection thus limiting possibility of hacking the account either by cracking a password or spear phishing[9]. The following are some of the common deployments of MFA.

A. One-Time-Password (OTP)

OTP is one of the popular deployed MFA method, some businesses use hardware based OTP while others use software based OTP. In OTP, the token, often in form a four or six digit number, is generated and used only once to login. In hardware based OTP, the token is provided by a pocket-sized device that can either be connected to the computer by USB, audio port or without any connection.The USB/audio based devices store shared secret which is used to generate tokens which are then entered in sites' login pages. Connectionless OTP devices have a LCD display and shared secret which they generate tokens through a challenge user must pass.RSA's secureID and Semantic's VIP are some of the leading hardware based OTP solutions[10].

Modern deployments of OTP are software based where token is generated by software engine, basing on previously provided user information, and sent to the user through out-of-band forms including email,sms or by phone call. In other adoptions, special mobile apps such as Google authenticator app are used to generate tokens that are used in a web authentication process. Google, Facebook, Apple and Dropbox are some of the sites deploying software based OTP though sms and mobile app[11].

Advantage of OTP solutions is that they reduce a risk of attacks due to stolen or cracked passwords[12]. They are also flexible in being integrated to businesses' platforms and customized to fit specific needs. However, deployments of these solutionsare costly to both businesses and consumers in terms of new hardware device to each user, token generator software and expenses for training users on the use of token generators [12]. Another downside is that OTP is not enabled by default in some sites including Google and Dropbox, meaning users who are not aware of the method will not be able to benefit from OTP's protection [13]. OTP with sms as out-of-bound form does not provide a completely safety as man-in-the-middle(MiTM) attacker can hijack token sent through sms and then use to authenticate in a site.Also, through man-in-the-browser (MiTB), an attacker can inject a trojan horse in the browser, through known browser vulnerabilities, allowing user to get authenticated through MFA and then modify transactions made by the user [14].

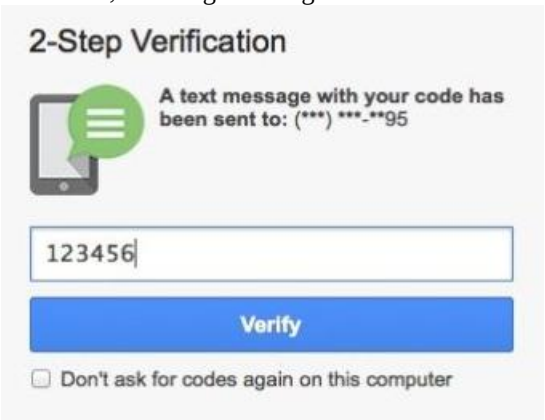


Figure 1: Google's OTP with sms

Figure 2: Hardware based product SecurID with a token

B. Smart Cards and Biometrics

Use of smart cards for MFA is popular in some businesses. In this approach, card reader is connected to either the computer or a smartphone and then a smart card containing user identification factors such as password and fingerprint is inserted and automatically authenticate a user[15]. In other deployments such as Barclays bank's PINsentry[1], a debit or credit card, instead of smart card, is used to generate a token which is then entered in a web login page for authentication. Biometric authentication is growing in its importance in protecting against online frauds. In this case, a scanned fingerprint, iris or voiceprint, using a provided hardware device, is used to provide an extra MFA layer to complete site

[1]http://www.barclays.co.uk/Helpsupport/HowtousePINsentry/P1242560253457

authentication[16]. Advantage of the method is that user does not have to remember any password to effectively make use of it. Also there is a little chance that user's biometrics can be stolen or lost. But there are several downsides of the method; its deployment is initially costly in terms of user devices and the whole set up of the application[17]. Biometric features may get damaged due to accidents or health issues such that application may fail to identify the same person. Since biometric features are stored in a database, hacking of the database application can expose the features and attacker is able to get the features and replay them to access their owners' accounts[18].

A biometric processing, if applied to many users at once, may become noticeably slow to affect the performance of the applications. Another critic is that feature like fingerprint can be easily be captured by sticky tape and then replicated for false use. The other downside is that the methods do have significant rates of false rejects and false acceptanceswhich may hugely affect effective use of applications such as internet banking [19].

III. BROWSER ENCRYPTION TECHNOLOGIES

A. HTTPS Protocol

HTTPS is a HyperText Transport Protocol (HTTP) that uses Transport Layer Security (TLS) cryptographic protocol to secure its traffic [20], [21]. TLS, formerly known as Secure Sockets Layer (SSL), is incorporated in web browsers to ensure confidentiality, message integrity and entity authentication are achieved between client's browser and a server hosting the application [20], [22]. Confidentiality is attained through encryption of data from the sender using standard cryptographic algorithms such as Advanced Encryption Standard (AES) [20]. Message integrity means ensuring that a message sent by sender reaches to the receiver without any modification that could be performed along the way [20]. Entity authentication is the way a client use to confirm the originality of the server before establishing a communication [20].

Entity authentication is achieved through the use of SSL certificates. Certificate is a unique online identity given to a business hosting an online service by a Certificate Authority (CA), after being approved as a genuine company and owner of the domain name [20], [22]. The certificate contains information including name of the company, its domain name, validity dates, unique public and private keys and the CA provided it [20].

When a client initiates a connection to the server, the client checks against the certificate of the server if, for instance, the company owns the accessed domain name, it a genuine business and its certificate is still valid [20], [22]. Once the check is passed successfully, the connection is established and data exchange is performed in encrypted form using the agreed encryption algorithm and public/private keys [20], [22]. A web page which is in a TLS-enabled HTTP connection with a server shows two indicators in a location bar, one being its URL beginning with *https* instead of *http*and also shows a closed padlock [20], [22].

This technique mainly prevents user, who is able to identify the two indicators, from falling to MiTM and pharming. Howeverthe effectiveness of this approach has been into questions since studies have revealed that most of online users do not know about these indicators and those who are aware of the indicators tend to ignore them and proceed to access the warned web pages [23],[24]. Also, phishers have been observed to design and place fake location bars with the two indicators on top of their phishing sites or placing closed padlock in a content part of the fake sites such that users aware of the two indicators can be easily fooled [22], [23].

B. Extended Validation SSL Certificate

Extended Validation SSL certificate (EV) is an improved SSL certificate required to be deployed by businesses to improve customers' confidence on their originalities. EV was designed in 2007 by CA/Browser forum (CAB)[2], a voluntary group of CAs, web browser vendors and suppliers of applications using digital certificates. A key improvement in EV is that any entity requesting for a certificate must be approved by the CA according to the issuance guidelines provided by CAB [25], [26]. The guidelines require CAs to;

- Verify legal identity as well as the operational and physical presence of website owner.
- Establish that the applicant is the domain name owner or has exclusive control over the domain name.
- Confirm the identity and authority of the individuals acting for the website owner, and that documents pertaining to legal obligations are signed by an authorized officer.

The guidelines also require CAs issuing the EVs to undergo EV auditing by a third party auditors recommended by CAB through audit programs such as WebTrust EV program audit [27]. Web browsers display enhanced indicators for EV on their address bars. These include name of the entity owns the certificate, change in color (green for address bar or URL text if the certificate is valid) and a closed padlock icon [28]. When entity's name is clicked, certificate information is displayed including name of the entity, domain name of the host, CA and certificate's period of validity.

As the process of obtaining EV SSL certificate limits fake companies from obtaining them, phishing attacks through launching of rogue sites are limited as well. However, the approach does not evade phishing completely because there isstill a significant number of businesses that are yet to deploy it in their websites[5]. Also, more than 70% of online users do not know about the EVs and their indicators. The other major shortcoming is that phishers take advantage of other site vulnerabilities to inject phishing codes (such as fake user login dialogue box) in an EV protected site thus still able to lure even users looking for EV indicators[29].

[2] https://cabforum.org/

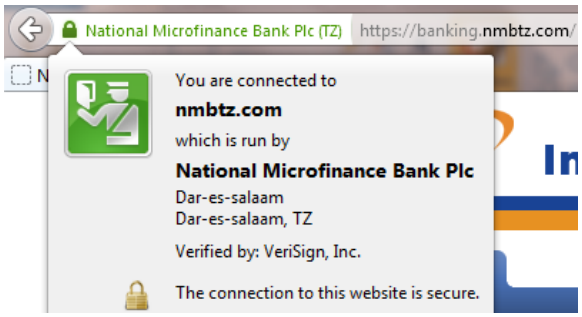


Figure 3: EV certificate and other indicators displayed when EV protected bank site is visited

IV. BROWSER ANTI-PHISHING TOOLS

A. Browser Anti-phishing Built-in Features

All browsers(Internet Explorer, Firefox, Google Chrome, Safari and Opera) have an anti-phishing feature known as Domain Highlighting. It highlights the domain of the current viewed page in the address bar with black color while the rest part of the URL is grey colored (see figure 3). This enables users to easily identity the true domain of the site they are visiting and can provide a clue of phishing sites. The browsers also support the use of https and EV SSL digital certificates. To enable users to always use the up to date browser with fixed known vulnerabilities, all browsers have an auto update feature which update the browser every time a user launches a browser with internet available. Below are browsers unique anti-phishing features.

1) Internet Explorer

Internet Explorer (IE) versions 8,9,10 and 11 have an anti-phishing tool known as SmartScreen filter which protects users against phishing sites and malware downloads[30]. The filter deploys a frequently updated black list of reported phishing websites kept by Microsoft and a set of heuristics which trace general characteristics of phishing websites' URLs to detect phishing websites[30]. If a web page's URL is found to be in the black list or web page contents have phishing behaviours, the browser blocks the access and recommends the user to return to a home page. If the filter is suspicious on the reputation of a site, it asks user to confirm the site's reputation before allowing user to access the site[31].

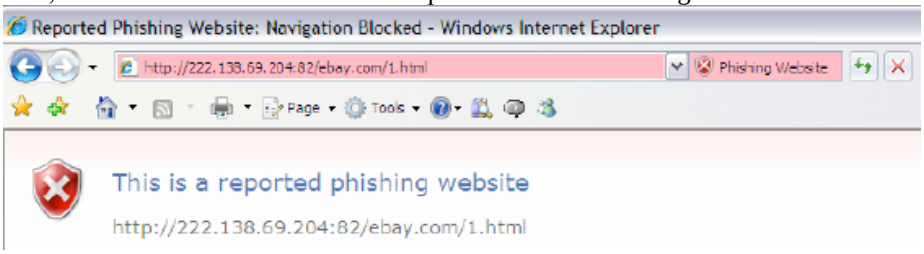


Figure 4: IE blocking a phishing site with a warning

TheSmartScreenalso has an anti-malware filtering capability[31]. The filter blocks access to a web page whose URL is found in a frequent updated blacklist database of URLs reported to contain malicious codes. The filter also works with a download manager to block downloads from sites which are in a black list or with phishing behaviours. IE v8 to v11 have a cross-site scripting (XSS) filter that provides protection against XSS attacks. It scans all server responses and if appear their requests are generated from other pages apart from which the user is currently accessing, the filter blocks the page and display an alert [32].

IE latestversions control downloading ofactiveX objects, which are vulnerable to malware injections, through the use of built-in activeX filter. When enabled, the filter blocks activeX objects from untrusted sites while gives user option to allow them to run from trusted sites. This in turn reduces the risk of installing malware if user is accessing a suspicious site[33].

Inprivate browsing is one of the security feature introduced from IE v8 onwards to provide a browsing environment where session data including usernames and passwords, form data, cookies, temporary internet files, history and form data are prevented from being saved in a hard disk[30]. Risk of phishing attacks through installed malware sniffing these data can highly be reduced when this feature is used.

Tracking protection[3] is another privacy protection feature in IE v9, v10 and v11 that prevents third party sites from tracking user online behaviours when user accesses a primary site. Only trusted third party sites registered by the user in the tracking protection list can be able to access user's data. Malware injections through images, ads, analyticsand others from phishing compromised sites can be limited with this feature enabled.

Also IE allows user to define sites in four security zones namely internet, local intranet, trusted sites and restricted sites and set general default levels of security accordingly. For a site defined in restricted zone, for instance, user can set IE not to install activeXobjects or run any script whereas for the sites in trusted zone, IE can be allowed to do so [34].

[3]http://windows.microsoft.com/en-us/internet-explorer/products/ie-9/features/tracking-protection

2) Mozilla Firefox

From version 2, Firefox has a built-in phishing and malware protection feature which checks against the lists of phishing and malware containing sites. When a user access a page, the feature, which is on by default, compares the site's URL against the Google's phishing and malware blacklists to determine site's safety. If the site is in a black list, a page is blocked and a warning "Reported web forgery" appears if it is a phishing site and a warning "Reported attack page" appears if it is a malware page. The browser uses Google's Safe Browsing protocol to automatically download and update the lists in every 30 minutes[35], [36].

When a file is downloaded from the site, the feature checks its signature against the updated list of known safe publishers to either block or allow the download. If the signature is not known, the browser sends the file's metadata to safe browsing service which will analysis and determines the level of safety of the file[35].

Pop-up blocker is another anti-phishing feature in the browser which is on by default [36]. It blocks all pop-up windows which in turn can prevent pop-up windows from compromised or phishing sites requesting login credentials.

Do Not Track is a feature that inform sites that they should not track a user on any information. However, this feature does not enforce sites in any ways such that sites have been observed to continue tracking even when the feature is on [37].

3) Google Chrome

The browser has a built-in anti-phishing and malware protection using Google's safe browsing technology. A visited site is always checked against a database of known phishing and malware hosting sites. If the site matches a phishing or a malware site, an access is blocked and a message 'Reported phishing website ahead' or 'Danger: Malware ahead!' are displayed respectively[38]. If the site does not match, safe browsing service analyzes characteristics of a site and if they are close to the phishing ones, the site is blocked [38]. The feature is enabled by default. The safe browsing also checks for a URL in the digital certificate of the visited site against the URL from the actual web server. If they do not match, the warning 'This is probably not the site you are looking for' is displayed[39].

Sandbox[4] is a feature in Chrome that limits the programs running from one tab to access other tabs ormodifya system. The tool protects XSSattacks, tracking of browsing activities and machine controlling by phishers[40]. Through Incognito surfing feature, user can maintain private browsing where by tracking information including cookies is not stored in a hard disk after sessions are over. Do Not Track feature is also existing in Chrome as in IE which when enabled, asks sites not to track user's browsing behaviours.

Chrome has built-in XSS and clickjacking filters. The XSS filters out any script that is about to run on a web page and is also present in the request that fetched that web page[41]. Clickjacking filter uses x-frame options to allow sites to filter out hidden buttons or forms placed by phishers on top of similar elements on a genuine web page[41].

4) Safari

Safari is known to have one of the best anti-phishingfilterscompared toother browsers[42]. The filter blocks all known phishing sites from the phishing blacklist and any sites which has similar characteristics to the phishing sites. Safari automatically prompts for approval before downloading files, and in doing so, it prevents some high-risk files from being executed before downloading[42]. The browser has a built-in pop-up blocker, preventing pop-up windows from potentially hijacking user's credentials.

The browser has a built-in sandboxing feature which protects programs running from one tab to access data in another tab or the system's hard disk[43]. The feature extends to plug-ins common to malicious attacks including adobe flash player, Silverlight, QuickTime and Java where each runs in a restricted environment, preventing any of their process from interfering other programs or the system[43]. Also certain plug-ins can be chosen by user to run from trusted sites only.

Safari, by default, prevents third party sites from leaving data including cookies in a machine's cache, local storage or databases [43]. With private browsing feature turned on, Safari stops storing browsing history, searches and online forms data. The browser also has a Do Not Track feature which when enabled, it asks sites not to track any of the user's information[43]. Safari also automatically sends Do Not Track requests when user uses private browsing.

5) Opera

Opera's fraud and malware protection feature filters any visited site having a match in Opera's phishing and malware blacklist database. The browser has a pop-up blocker to filter out pop-up windows[44]. It provides a Do Not Track[5] option which if enabled prompts sites not to track the user on online activities. The browser has a cookie management feature that user can use to opt which site to and not to accept cookies[44]. Opera's private browsing[6] allows user to browse a site without history, cookies, and forms data being saved when a tab is closed.

Generally, browsers built-in anti-phishing features especially those which are default enabled help users to get automatic phishing protection regardless of degree of phishing awareness of users as well as without the need to install third party tools. Auto update feature in most browsers enforcesimmediate patching of vulnerabilities without users' knowledge, reducing risks of zero-hour exploits. With frequently improved blacklists database and phishing heuristics, anti-phishing filters have also been improving in their efficiency to detect phishing attacks[45].

[4] http://tools.google.com/dlpage/res/chrome/en-GB/more/security.html

[5] http://www.opera.com/help/tutorials/security/control/

[6] http://help.opera.com/Windows/12.10/en/private.html

However the browser features still face many shortcomings. Not all attacks in the wild are reported. Many phishing attacks exist in few hourswhile most are launched from compromised machines[46]. This weakens effectiveness of blacklists. Features such as SmartScreenwhich are disabled by default do not help majority of user unaware of phishing and anti-phishing tools. Most of the browsers, when blocking malicious sites, still allow users to disregard the warnings if they wish. As many users often tend to ignore phishing warnings, this design still exposes users to phishing.

B. Browser Anti-phishing Plug-ins

Anti-phishing plugins are useful in providing extra security features that are not offered by most browsers. They have proven to offer a very high detection rate (up to 96%) of phishing sites while provides extensive information and indicators about the safety levels of sites/domains helping users to browse with cautions[47]. Some of them offer multiple roles thus preventing attacks from different vectors, for instance, as anti-phishing filter as well as ads blocker[47].

The tools, however, are limited with ability to capture zero-day phishing attacks as most of them depend on blacklists. Their indicators on the safety levels of sites are useless for users who do not know how to use them or unaware of phishing. Most of the warnings are passive and for those which are active, they still offer to users, options to ignore warnings thus not enforcing protection.

1) Anti-phishing Filters

These tools use two approaches to filter phishing sites; blacklists and heuristic features of phishing sites. Blacklist-based plug-inidentifies and filters out or alerts user on phishing sites if they exist in frequently updated databases of reported phishing sites found in the wild[46]. The blacklists host URLs of known phishing sites or sites known to contain malicious codes. The databases are often maintained by plug-in developers, their partners and/or their user communities [46], [47]. Examples of the filters are Netcraft,TrustWatch and EarthLink toolbars.

Heuristic-based filters deploy machine learning algorithms or rules on URLs or contents characteristics of sites to trace and block or alert sites appear to be close to phishing behaviours[46]. Netcraft and SpoofGuard[7] are some of the toolbars falling in this category using rule-based heuristics.

Netcraft[8] is a toolbar almost for every major browser, deploying both blacklist and heuristic methods. When a visited site is in a blacklist, the tool blocks the access with pop up warning message recommending user to cancel the browser[47]. It has a risk rating gauge which turns red to alert user the site has some characteristics of phishing sites otherwise turn green for a clean site.

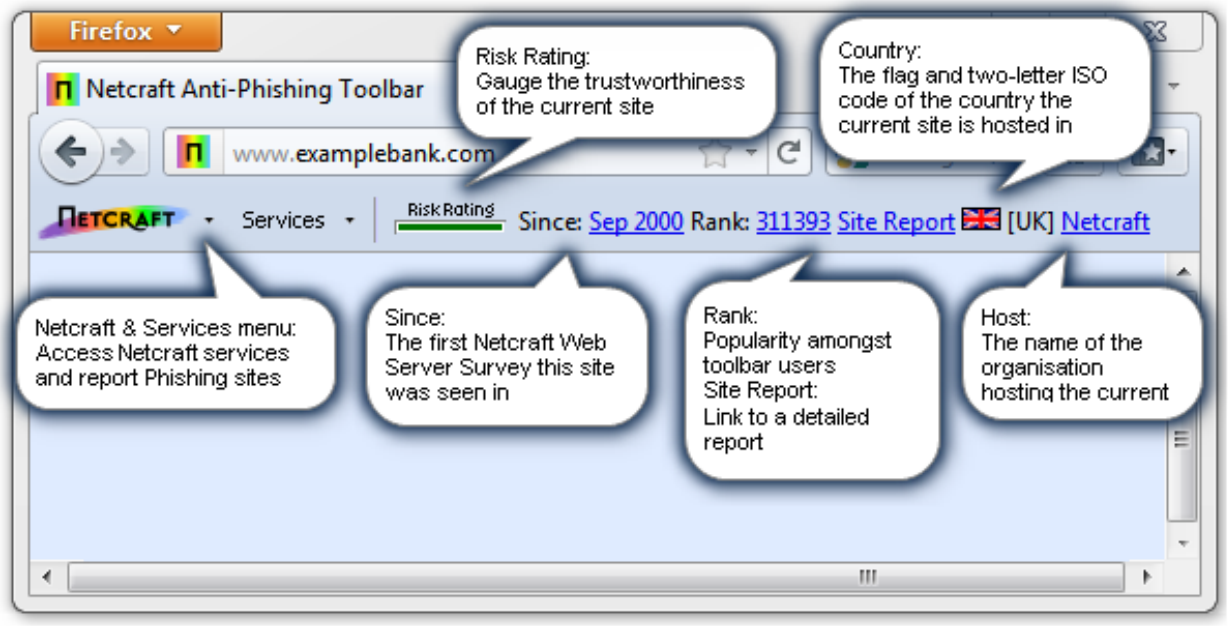


Figure 5: Netcraft toolbar with its indicators.

2) Scripts Blockers

These are tools that block JavaScript, Java and other executable web contents from running when primary or third part sites are loaded [48]. Scripts are one of favorite loopholes used by hackers to launch attacks such as XSS, drive by downloads, cross zone DNS binding, router hacking and other clickjacking attacks[48], [49]. NoScript (for Firefox) and NoScripts (for Chrome) are examples of typical plug-ins.They use a whitelist approach where user assigns trusted sites to allow their scripts to run while scripts from all other sites not in the lists are blocked accompanied with notifications [49]. Other script blockers include ScriptSafe, FlashBlock and ScriptBlock.

[7] http://crypto.stanford.edu/SpoofGuard/
[8] http://toolbar.netcraft.com/

Figure 6: NoScript blocking scripts from a site

3) Advertisement Blockers

Phishers are known to be injecting malicious advertisements (ads) on compromised sites to launch drive by download attacks[50]. Ads blockers are useful to prevent these attacks by blocking scripts running any adin form of banners, pop-ups and video ads [48]. Some of them provide an option of assigning trusted domains whose sites are allowed to display their ads. Ad blocker such as AdBlock Plus[9] (for Firefox, Chrome, Opera, safari and IE) provide further capability of being able to block known malicious ads from a blacklist of malicious sites [48]. Other[10] ad blocking plug-ins includesSuper Ad Blocker, Google Toolbar and ZeroAds.

4) SessionsEncrypting Plug-ins

Plug-in such as HTTPS Everywhere encrypts all site traffic between user and a site server. The tool helps to overcome weakness of some sites from encrypting login credentials only leaving other information as plain texts [51]. Using a hacking tool such as Firesheep, in such a case, user data can easily be sniffed in Wi-Fi environments [51]. Other similar toolsare WordPress HTTPS plugin[11]for WordPress sites and Force-TLS

5) User Tracking Blockers

These are the tools that block sites from tracking user's online behaviours. Disconnect[12] is an example of the plugins which block cookies and prevent sites from tracking browsing history and searches in web and search engine. It helps user to visualize which invisible tracking requests are coming from and user can opt which sites to allow tracking [49].

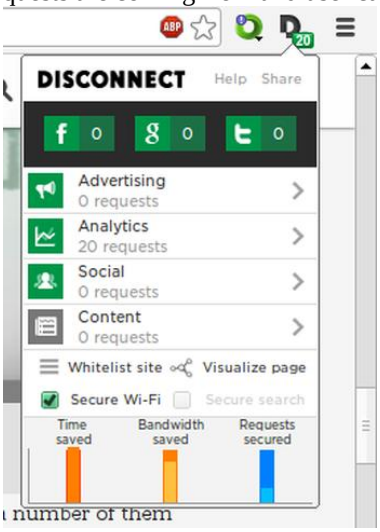


Figure 7: Disconnect plug-in showing blocked tracking requests

6) Password Managers

Browsers provide a feature to store web passwords in a web cache. However, this feature does not provide strong security such that using some hacking tools or when hacker gets an access to user's machine, all passwords can be easily exposed [52]. For instance, Chrome, Safari, Firefox and IE allow whoever with an access to the machine to view all web stored passwords asclear texts[52].Most users, in the fear of forgetting passwords, tend to use common passwords in many sites and email platforms, making them vulnerable in diversified attacks once the passwordsare hacked.

With a password manager plug-in, all web passwords can be securely preserved, using advanced encryption algorithms, under one database with one strong master key.Even if a hacker gets an access to the machine, he has also to have a master key to access all stored passwords thus providing an extra security layer to breach.The plug-ins help users to overcome the challenge of remembering passwords through the use of common passwords by allowing unlimited unique passwords to be securely stored. LastPass, keePass and 1Password are common products in this category.

[9]https://adblockplus.org/blog/blocking-malicious-sites-with-adblock-plus
[10]http://www.pcworld.com/article/139515/article.html
[11]http://www.wpwhitesecurity.com/wordpress-plugins/wordpress-ssl-setup-login-wordpress-https-ssl-plugin/
[12]https://chrome.google.com/webstore/detail/disconnect/jeoacafpbcihiomhlakheieifhpjdfeo?hl=en-US

7) Safety Indicative Information Providers

Some of the tools are designed to provide cautious information to users and depend on them to makejudgments on the safety of the sites.Netcraft, for instance, has a risk rating feature[13] that shows high risk level (with red colored sign) if the site has some phishing characteristic or hosted in a known compromised domain/server otherwise the site is safe (shown with green color indicator)[47]. The other feature[14], country flag and a two letter ISO country code, indicates where the domain is hosted (see figure 5). A domain such as Barclays.co.uk is not expected to be hosted in Russia thus such information can raise an alert to the users on the site's originality. Similar toolbars are McAfee SiteAdvisor, TrustWatch, WOT and SpoofGuard[47].

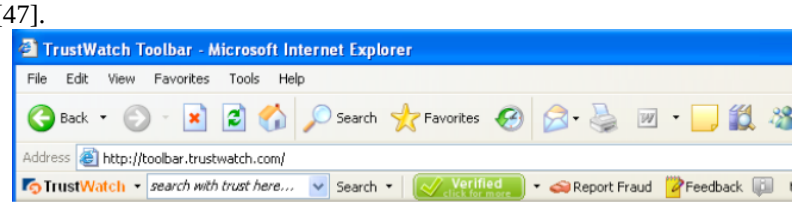


Figure 8: TrustWatch toolbar verifies a site with a green flag labeled "Verified"

V. ANTI-MALWARE SOFTWARE

A. Antivirus

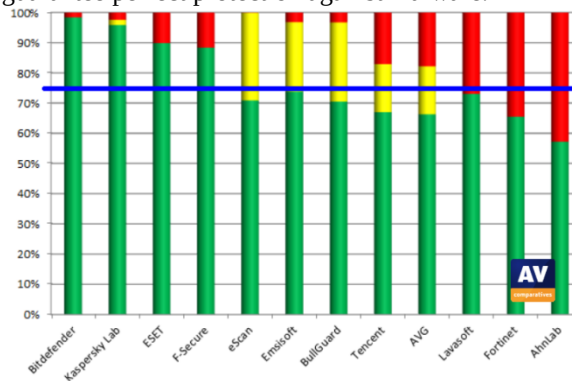
Antivirus (AV) is a software that attempts to identify, neutralize and remove malicious programs in a computer. Most of AVs have default configuration of automatic scanning for viruses in incoming files to the system, for examples, email attachments and web downloads, or files, already in the system, when they are opened, closed or executed[20]. Scanning on demand is another common option provided. The software can scan a number of critical areas of computer systems including system memory, registry, operating system files and programs' files [53]. AVs use mainly three methods of detecting malware; virus dictionary, tracing of suspicious behaviors and heuristics analysis.

Virus dictionary is a database of all known virus signatures reported in the wild.AV checks codes of a file or portion of it if contains similar codes of known signatures. Signature could be a series of bytes or cryptographic hash of the file or its portion[54]. If matching, AV attempts to delete the file, remove the virus infected portion or quarantine the whole file [55]. AV can also trace behaviors of programs in the system to look for any suspicious activities which are similar to those of malware. For instance, when a system executable file is being modified by unrelated program, then the antivirus can suspect as a malicious activity and sends out an alert to the user [56].

In heuristic analysis, AV looks for generic attributes of the viruses in other programs, often by emulation approach such as sandbox. In this approach, AV emulates the host system and run the suspicious file codes to detect virus attributes such as self-extracting codes or codes trying to invoke other executables files[56], [57]. If many virus attributes are found, then the file will be blocked from accessing a real system.

AVs come in two forms of services, host-based and cloud-based virus detections. In host-based, virus signatures are downloaded to the host and virus detection analysis is done in the local machine. In cloud-based, characteristics of the scanned file are sent to the vendor-hosted cloud service, consisting of detection analysis engine and a database of signatures, where the detection processing is performed[54]. The former is significant in offline environments but is limited with an access to the current (online) AV database. Cloud service ensures real time protection by up to date and comprehensive online database of virus signatures and heuristics collected from multiple systems of vendor community [54].

Recent studies by AV-Comparatives have shown that some AVs are performing well in malware protection. 7 out of 13 dominant commercial AVs had a more than 84% proactive protection rate (in an offline heuristic/behavioral test) with few false alarms and low false negative rate[58]. In a detection test by signatures, 6 AVs had a detection rate of at least 99%[59]. However, other AVs had proactive protection rate and detection rate as low as 57% and 89% respectively which show that AVs only do not guarantee perfect protection against malware.



Key:*Green = blocked/protected; Yellow = user dependent; Red = not blocked/compromised*

Figure 9: Results of 2014 Antivirus comparative proactive test

[13]http://toolbar.netcraft.com/help/faq/

[14]http://toolbar.netcraft.com/help/faq/

B. Anti-phishing Software

Most of AV vendors have integrated anti-phishing filters in their AV suites, as plug-ins or suite-embedded components. Some filters use vendor community's blacklists while others use also heuristic analysis to block phishing sites. Other filters[15] scan and prevent downloads from sites known to host malware, not only through browsers, but also through chatting applications(such as yahoo messenger and MSN)and peer-to-peer applications. Other filters such as Norton's Safe Web[16] can scan for URLs in user's social media sites and block those directing user to phishing sites or malware downloads.

Figure 10: ESET Smart Security blocking a phishing site

AV-Comparative's 2014 study revealed that 11 of 12 AV suites scored more than 80% of blocked phishing sites rate with only few false alarms. This shows that AV anti-phishing solutions, though they are relatively new, are performing almost at the level of other standalone anti-phishing plugins. This could be due to large and established AV vendors' communities.

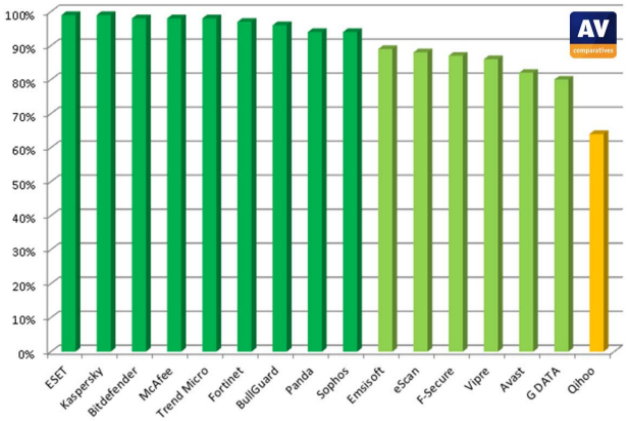


Figure 11: Comparative performances of AV suites' anti-phishing filters in blocking phishing sites

C. Anti-Spyware

These are software that track, repair, quarantine or remove spywareincluding key loggers, screen loggers, Trojans, hijackers, dialers, rootkits and backdoors[20]. Anti-spyware uses blacklist and/or heuristic/rule-based approach to filter spyware on demand or on real time basis. Blacklist is a vendor's database hosted that contain spyware signatures observed in the wild. In heuristic/rule-based approach, known characteristics of spyware such as certain setting changes in window registry or browser, are used to predict unknown intruders. Anti-spyware scans common areas such as system memory, window registry, browser cookies, bookmarks as well as operating system and program files to analyze spyware traces [53]. Anti-spyware provides option of quarantining or deleting detected spyware. Most of the leading anti-spyware solutions are integrated in AV suites, for instance, Bitdefender, Norton and Kaspersky products.

VI. EMAIL FILTERS

Email filtersidentify and isolate both spams and phishing emails from being read by users. Several combined techniques, as described below, are often deployed in one filter to enhance true positives and minimize false positives. For instance, MailWasher, Spam Bully andCleanMail email client filtersuseblacklists/whitelists, image blocking and classifier techniques,among others. Most email client filters have an ability to block, delete or quarantine a confirmed malicious email.

[15]http://us.norton.com/products/tutorials/tutorials.jsp?pvid=n3604&tutid=download_insight
[16]http://us.norton.com/internet-security/

Filters using few techniques are disadvantaged because of individual weaknesses of the techniques. Blacklist and signature based approach lags behind zero-day scams as new altered attacks are produced every day. Classifiers and content filtering are known to generate significant false positives[60]. Sender authentication becomes useless when email scams are generated from the comprised legitimate machine[60].

A. Blacklist and Whitelist

This is a technique that is deployed at the server or client sides. Ablacklist database, managed by a vendor, mail administrator or user, hosts email addresses known to be sending malicious emails. A list depends on the reported cases by email users, administrators, vendors' business partners and anti-spam campaigners [20]. Most mail applications have a tool that allow user to report a sender to its local blacklist or vendor hosted. In other deployments, a blacklist can be of IP addresses of machines known to be spams relays/proxies or URLs, domains and IP addresses of machines known to host phishing sites [60].When an incoming email is known to be from one of the sender from the list, email client can either block it or locate it in the junk/spam folder. Other email applications use also whitelists in whichuser or administrator can specify trusted senders allowed to receive emails from [20].

B. Classifiers

Use of machine learning algorithms to predict safety of the incoming emails is very popular in email filters. Word based classifier such as Bayesian is one of the common email classifiers. The filter computes cumulative probabilities of all words for each spam and malicious email from a comprehensive database as a training set and then determines a spam threshold value. The value for each incoming email is then computed and compared with the threshold value to determine its safety level [61]. Training set can be collected at the user, administrator or vendor community levels.SpamGuard is an example of the classifier that is used by Yahoo mailand as an add-on to Microsoft Outlook.

C. Signature and Checksum Filters

In this technique, signatures of spams identified by email users are computed and then stored in a shared database. For every incoming email, its signature is determined and then compared with those in the database and if matched, the email will be flagged[62]. In other implementations, a database of computed checksum from confirmed spams is used instead of signatures [62].

D. Content Filtering

In this type of filtering, regular expressions known to be common to spammers and phishers, such as Viagra, bank account, username, are examined and used to flag spams[20]. Also emails with headers which appear to be violating RFC 5322 standard are also rejected. Emails come with uncommon file extensions such as .exe, which are known to be used for malware distribution, are often subject to blocking by some email applications. Filtration of links is also common where URLs are examined to identify if they are contained in the blacklists of phishing sites [60]. Hyperlinks from untrusted sources are also disabled in other filters by default [60].

E. Image Blocking

Malicious emails are also known to be containing malware injected images. Many email clients such as Yahoo and Gmail provide a default setting of blocking all images in the email content. Users, though, are given options to display the images once are certain of their senders.

F. Sender Authentication

To prevent sender from forging their email addresses to look like they are coming from genuine domains, most email applications deploy sender authentication methods using Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) technologies. In these approaches, each domain's owner publishes, in the DNS, IP addresses of all of its machines that are allowed to send emails using its domain name. Upon reception of the email, the receiving email server or client, checks in the DNS if the sender's claimed IP address is in the list and if not, the email is regarded as a forged one[20]. To enhance efficiency of the protocols, Domain-based Message Authentication, Reporting & Conformance (DMARC)[17], a set of procedures, was later integrated which added feedback to sender what receiver should do when an email is not authenticated.

Use of visual image is also deployed as an authentication approach. In this case, sender's image is incorporated into the email header as part of the email application user interface[63]. When user opens an email, he can confirm the sender by seeing his image. Image at this location is difficult from being spoofed unless the application's interface is altered [60].

VII. ANTI-PHISHING TRAINING TOOLS

Educating users on phishing is regarded as one of the most effective anti-phishing strategy. There are a number of tools today which offer facilities to train user on awareness of phishing. The training software contains a database of real world phishing emails in which the administrator can pick any and then send to a group of users and trace their responses [64]. If a user falls into a phishing trap by clicking to a fake link, is immediately warned with a message explaining what was

[17]http://www.dmarc.org/overview.html

wrong with the links. With extensive reporting features, administrator can be able to analyze which users failed and in what areas so as to design appropriate training programs. A study by [64] suggests that at least two such exercises are needed to ensure users retain the phishing knowledge for a longer period.

In a tool such as Anti-phishing Phil[18], user is engaged in a game in which the tool displays different URLs that user has to respond which are real and fake ones. User is then given immediate feedback and if failed, is automatically enrolled to a short online training. Other tools including PhishProof[19] and ThreatSim[20] offer also video based training sessions that administrator can register their users to undertake the lessons. The lessons are about real world phishing emails and how to identify and evade them.

With at least two phishing tests performed to users at a short interval, these tools have proved to be very effective such that they can reduce susceptibility rate of up to 84% [65]. Game based training has shown to have higher impact compared to online training sessions while has also attracted more users to engage in training [64].

VIII. PROPOSED ANTI-PHISHING TOOLS

A. Content Filtering

[66] developed CANTINA, a content based phishing detection toolbar, that analyzes web page content to determine whether the page is a phishing one or not. It computes Term Frequency-Inverse Document Frequency (TF-IDF) of each term and then searches in a search engine the 5 terms with the highest TF-IDF values. If the domain of the web page is among the n domains of the returned search results, then the site is legitimate otherwise a potential phishing one. To reduce false positives, the toolbar uses five other heuristic rules; domain age, dots in URL, suspicious characters in the URL, links in the content and existence of forms. It achieves a detection rate of up to 97% of phishing sites.

B. Visual Similarity

A solution by [67]addressed a phishers' technique of mimicking a HTML page by using an image to evade HTML based filters. The browser takes a snapshot of suspected site and compare against a whitelist of sites such as PayPal, eBay, Amazon and banks that are likely to be targeted by phishers. Using Harris-Laplace and k-means clustering algorithms, silent features of the snapshot are analyzed and compared against those of whitelist sites. If there is image matching as well as their URLs, then a site is legitimate otherwise it is a phishing one. Up to 98% accuracy is achieved with a less than 1% of false positives and negatives.

C. Data Mining

There are many proposed email anti-phishing solutions deployed data mining techniques. One of them is R-Boost by [68] which used a combination of C5.0, k-NN (k=3,4) and SVM clustering algorithms to establish a final classification of the email. R-Boost use five heuristic features to enable each classifier to determine the email class, either phishing or non-phishing. Voting is then done to establish which class has been most determined by the three classifiers, which then represents the final class of the email. Each algorithm develops its classification model through a provided training set. The heuristic features used are; presence of IP address in the email URL, email format in HTML, presence of JavaScript in the email, number of URLs and maximum number of periods in the URLs.

D. Heuristic based

[69]proposed anti-phishing email filter called Phishwish which based on 11 rules to identify phishing emails. The tool is applied to emails directing user to login to a website. The rules are categorized as; identification and analysis of the login URL in the email, analysis of email headers, analysis across URLs and images in the email and determining if the URL is accessible. Each rule is given one score if applicable otherwise is given as 0. Weighted mean of all rules is computed to determine the email score. If the score is greater than 50% then the email is labelled as phishing otherwise it is a clean one. The testing results of the tool showed that it outperformed other common anti-phishing email filters such as SpamAssassin and Google's browser based anti-phishing filter.

E. Blacklist

PhishNet is a solution suggested by [70]which developed a predictive blacklist from a known blacklisted phishing site URL structure. Child URLs were generated by varying the URL structure of the blacklisted URLs using five heuristic features; varying top level domains (TLDs), URLs pointing the same IP address, exchanging filenames for URLs with similar directory structure, exchanging query string for URLs with similar directory structure and varying brand names in the same URL structure. The established child URLs were then tested to eliminate non-existent and non-phishing sites and produce a predictive blacklist of 18,000 URLs from 6,000 parent URLs. The tool produced very few false positives and negatives.

F. Offensive defense

These are the tools that react to phishing attacks by automatically providing fake credentials, mixed with genuine ones submitted by victims, to phishing sites so as to distract phishers from ease data harvesting. The tools depend on

[18]http://www.wombatsecurity.com/antiphishingphil

[19]http://www.inspiredelearning.com/phishing_training/phishing_training_features.htm

[20]http://threatsim.com/

browsers' built-in or third party anti-phishing tools to detect phishing sites. Phishers needs to analyze the data and filter true data, the process which may take long time for phishing campaigns to be identified and taken down by authorities[71]. The fake data are designed with detectable behaviors in such a way that a phisher can easily be traced when visits a legitimate site's server to filter true credentials [72].

BogusBiter, for instance, is a toolbar installed at the end user designed to detect phishing sites and then provide bogus data, on user's behalf, to the sites[71]. Humboldt is a similar tool but fake credentials are coordinated from all distributed clients and not from a single client[72]. These tools, as downsides, are big bandwidth consumers, can cause denial of service (DoS) floods and do not detect non-standard HTML forms [46].

IX. CONCLUSION

Tests performed on most anti-phishing tools have shown that some tools can achieve phishing detection rates between 90% and 99% which representsa good achievement towards mitigating phishing. Recent increase in deployments of MFA indicates that the methods are perceived to be effective against credentials hacking and MiTM. Incorporated anti-phishing capabilities in anti-spam solutions have improved abilities of email applications to filter out not only spams but also phishing emails. Introduction of training tools in anti-phishing campaigns has helped organizations to increase phishing awareness to their staff thus mitigating the impact of spear phishing.

However, shortcomings observed in each solution has suggested that each can be effective in protecting users against particular phishing vectors but can be vulnerable to other vectors. MFA provides strong protecting against credentials hacking but is still vulnerable to MiTB. Blacklist based anti-phishing filters are effective against well reported phishing sites but are weak against zero day attacks. Warnings provided by most tools, after detecting phishing sites, gives user option to ignore them and proceed accessing the sites instead of completely blocking the access. Other warnings such as those given by some plugins are completely passive thus do not provide any enforcement to prevent ignorant users from accessing malicious sites. With some of the anti-phishing features such as those in browsers being disabled by default, users unaware of phishing and therefore importance of these features cannot benefit from them. Wide adoption of MFA is limited by cost implications and applications performance concerns in processing many users' credentials at once.

To effectively mitigate phishing, users need to deploy several anti-phishing solutions combined strategically to cover protection against most of the phishing vectors. For instance, user has to use a browser with all anti-phishing features enabled and installed with plugins that offer other uniqueservices such as ads, scripts and tracking blocking as well as password management. Best anti-malware software providing wide range of protection should be installed in a machine. For any site supporting MFA, user has to enable and make use of it. User should use email application installed with the best performing anti-phishing filter. Organizations and businesses must invest in training their staff and customers on awareness of phishing including the use of anti-phishing training tools. Anti-phishing solutions should incorporate more of heuristic and machine learning algorithms to effectively combat zero day attacks. Their warnings should completely isolate users from possibilities of accessing confirmed phishing sites.

REFERENCES

[1] Anti-Phishing Working Group, (2012), *Phishing Activity Trends Report 4th Quarter 2012*, APWG.

[2] Symantec Corporation, (2012), "2012 Norton Study: Consumer Cybercrime Estimated at $110 Billion Annually", *Symantec*. Available at: http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02 [Accessed September 2013].

[3] Symantec Corporation, (2013), *Symantec Internet Security Threat Report 2013*, Symantec Corporation.

[4] Lynch J., (2005), "Identity theft in cyberspace: Crime control methods and their effectiveness in combating phishing attacks", *Berkeley Technology Law Journal*, 20: 259-300.

[5] Nagunwa, T (2014a), "Assessing Usage of Web Browser Security Indicators in e-banking: A Case Study", *International Journal of Advanced Research in Computer Science and Software Engineering*, 4(9): 195-202

[6] Holbl, M., (2007), "Authentication approaches for online-banking", *Council of European Professional Informatics Societies (CEPIS)*. Available at: http://www.cepis.org/files/cepis/20090901104203_Authentication%20approaches%20for%20.pdf [Accessed December 2013].

[7] FFIEC, (2005), "Authentication in an Internet Banking Environment", *Federal Financial Institutions Examination Council (FFIEC)*. Available at: http://www.ffiec.gov/pdf/authentication_guidance.pdf [Accessed December 2013].

[8] Owen, N., (2006), "Reducing Online Banking Fraud with Stronger Authentication Methods", *Bank Info Security*. Available at: http://www.bankinfosecurity.com/reducing-online-banking-fraud-stronger-authentication-methods-a-115/op-1 [Accessed November 2013].

[9] Dubin, J., (2008), "Understanding multifactor authentication features in IAM suites", *Search Security*, Available at: http://searchsecurity.techtarget.co.uk/tip/Understanding-multifactor-authentication-features-in-IAM-suites [Accessed September 2014].

[10] Parizo, E., (2013), "Best of authentication 2013", *Search Security*, Available at: http:http://searchsecurity.techtarget.com/feature/Best-of-authentication-2013 [Accessed September 2014].

[11] Godorn, W., (2013), "Here's Everywhere You Should Enable Two-Factor Authentication Right Now", *Life Hacker*. Available at: http://lifehacker.com/5938565/heres-everywhere-you-should-enable-two-factor-authentication-right-now [Accessed September 2014].

[12] Myerson, J., (n.d), "Pros and cons of multifactor authentication technology for consumers",*Search Financial Security*, Available at: http://searchfinancialsecurity.techtarget.com/tip/Pros-and-cons-of-multifactor-authentication-technology-for-consumers [Accessed September 2014].

[13] O'Reilly, D, (2013), "How to enable two-factor authentication on popular sites", *CNET*, Available at: http://www.cnet.com/how-to/how-to-enable-two-factor-authentication-on-popular-sites/ [Accessed September 2014].

[14] Paganini, P., (2013), "Man in the browser attacks scare banking world", *Security Affairs*, http://securityaffairs.co/wordpress/17538/cyber-crime/man-browser-attacks-scare-banking.html [Accessed September 2014].

[15] Search Security, (2011), "Security token and smart card authentication", *Search Security*, Available at: http://searchsecurity.techtarget.com/tip/Security-token-and-smart-card-authentication [Accessed September 2014].

[16] Search Security, (2011), "Biometric authentication know-how: Devices, systems and implementation",*Search Security*, Available at: http://searchsecurity.techtarget.com/tip/Biometric-authentication-know-how-Devices-systems-and-implementation [Accessed September 2014].

[17] UBWG (2002), *Use of Biometrics for Identification and Authentication Advice on Product Selection*, UK Biometrics Working Group

[18] Hisham, A., Sellahewa, H., Jassim, S., (2011), "Accuracy and Security Evaluation of Multi-Factor Biometric Authentication", *International Journal for Information Security Research (IJISR)*, March 2011, 1(1)

[19] Nuance, (2009), *Measuring Performance in a Biometrics Based Multi-Factor Authentication Dialog*, Nuance.

[20] Nagunwa, T., (2008), *Investigation of data privacy threats in online retail industry and assessment used in mitigating their impact*, MSc Thesis, Dublin Institute of Technology.

[21] Roessler, T., Saldhana, A., (2010), "Web Security Context: User Interface Guidelines", *World Wide Web Consortium*. Available at: http://www.w3.org/TR/wsc-ui/#sec-tls-indicator [Accessed November 2013].

[22] Stebila, D., (2010), "Reinforcing bad behavior: The misuse of security indicators on popular websites", *Proceedings of the 22nd Conference of the Computer-Human Interaction*, pp. 248-251. Available at: ACM Digital Library [Accessed November 2013].

[23] Dhamija, R., Tygar, J., Hearst, M., (2006), "Why Phishing Works?",*Proceedings of the conference on Human factors in Computing Systems (CHI-2006)*, pp. 581-590. Available at: ACM Digital Library [Accessed November 2013].

[24] Mannan, M., Oorschot, P.C., (2007), "Security and Usability: The gap in real-world online banking", *NSPW '07 Proceedings of the 2007 Workshop on New Security Paradigms*, pp. 1-14. Available at: ACM Digital Library [Accessed November 2013].

[25] CAB, (n.d), "About EV SSL", *CA/Browser Forum*. Available at: https://cabforum.org/about-ev-ssl/ [Accessed November 2013].

[26] GoDaddy, (2013), "Premium extended validation SSL: Overview", *GoDaddy*, Available at: http://www.godaddy.com/ssl/ssl-extended-validation.aspx [Accessed November 2013].

[27] CAB, (n.d), "Information for auditor and assessors", *CA/Browser Forum*. Available at: https://cabforum.org/information-for-auditors-and-assessors/ [Accessed November 2013].

[28] CAB, (n.d), "Information for site owners and administrators", *CA/Browser Forum*. Available at: https://cabforum.org/ [Accessed November 2013].

[29] Goodin, D., (2008), "Will EV SSL stop phishing attacks? Probably not", *The Register*, Available at: http://www.theregister.co.uk/2008/02/29/ev_ssl_doubts/ [Accessed August 2014].

[30] Brink (2009), "Windows 7: Internet Explorer SmartScreen Filter - Turn On or Off", *Windows Seven Forums*, Available at: http://www.sevenforums.com/tutorials/1406-internet-explorer-smartscreen-filter-turn-off.html [Accessed November 2013].

[31] Lawrence, E., (2008), "IE8Security Part III: SmartScreenFilter", *IE Blog*, Available at: http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-iii-smartscreen-filter.aspx [Accessed September 2014].

[32] Ross, D., (2008), "IE8 Security Part IV: The XSS filter", *IEBlog*, Available at: http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-iv-the-xss-filter.aspx [Accessed September 2014].

[33] Thurrott, P., (2011), Internet Explorer 9 Feature Focus: ActiveX Filtering, Available at: http://winsupersite.com/windows-7/internet-explorer-9-feature-focus-activex-filtering [Accessed September 2014].

[34] Posey, B., (2006), "New Security Features in Internet Explorer 7", Available at: http://www.windowsnetworking.com/articles_tutorials/Security-Internet-Explorer-7.html [Accessed September 2013].

[35] Mozilla, (n.d), "How does built-in Phishing and Malware Protection work?",*Mozilla*, Available at: https://support.mozilla.org/en-US/kb/how-does-phishing-and-malware-protection-work [Accessed September 2014].

[36] O'Donnell, A., (n.d), "Firefox Security Tips and Tools", *About Technology*, Available at: http://netsecurity.about.com/od/webbrowsersecurity/a/Firefox-Security-Tips-And-Tools.htm [Accessed September 2014].

[37] Muchmore, M (2012), "The State of 'Do Not Track' in Current Browsers", *PC Magazine*, Available at: http://www.pcmag.com/article2/0,2817,2402168,00.asp [Accessed September 2014].

[38] Google, (n.d), "Phishing and malware alerts", *Google*, Available at: https://support.google.com/chrome/answer/99020?hl=en [Accessed September 2014].

[39] Bradley, T., (n.d), "Google Chrome Security", *About Technology*, Available at: http://netsecurity.about.com/od/webbrowsersecurity/p/chromesecurity.htm [Accessed September 2014].

[40] Sylvain, N., (2008), "A new approach to browser security: the Google Chrome Sandbox",*Chromium Blog*, Available at: http://blog.chromium.org/2008/10/new-approach-to-browser-security-google.html [Accessed September 2014].

[41] Keizer, G., (2010)," Chrome apes IE8, adds clickjacking, XSS defenses", *Computer World*, Available at:http://www.computerworld.com/article/2523151/web-apps/chrome-apes-ie8--adds-clickjacking--xss-defenses.html [Accessed September 2014].

[42] Grims, R., (2009), How Secure Is Safari?,*PC World*, Available at:http://www.pcworld.com/article/158706/how_secure_is_safari.html [Accessed September 2014].

[43] Apple, (2014), "Safari: The smartest way to surf", *Apple*, Available at:https://www.apple.com/safari/ [Accessed September 2014].

[44] Spamlaws, (n.d), "Security of The Opera Browser", *Spam Laws*, Available at: http://www.spamlaws.com/opera-browser-security.htm [Accessed September 2014].

[45] Rubenking, N., (2013), "Browsers Beat Security Software in Phishing Protection Test", *Security Watch*, Available at: http://securitywatch.pcmag.com/web-browsers/307527-browsers-beat-security-software-in-phishing-protection-test [Accessed September 2014].

[46] Khonji, M., Iraqi, Y., Jones, A., (2013), "Phishing Detection: A Literature Survey", *IEEE Communications Surveys & Tutorials*, IEEE, 15(4):2091 – 2121.

[47] Cranor, L., Egelman, S., Hong, J., Zhang, Y., (2006), *Phinding Phish: An Evaluation of Anti-Phishing Toolbars*, CyLab - Carnegie Mellon University.

[48] Drager, D., (2011), "Five Best Browser Security Extensions",*Life Hacker*, Available at: http://lifehacker.com/5770947/five-best-browser-security-extensions [Accessed September 2014].

[49] Wallen, J., (2013), "Five must-have browser security add-ons", *Tech Republic*, Available at: http://www.techrepublic.com/article/five-must-have-security-browser-add-ons/ [Accessed September 2014].

[50] Nagunwa, T., (2014), "Behind identity theft and fraud in cyberspace: The current landscape of phishing vectors", *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 3(1): 72-83.

[51] Fitzpatrick, J., (2010), "Firesheep Sniffs Out Facebook and Other User Credentials on Wi-Fi Hotspots", *Life Hacker*, Available at: http://lifehacker.com/5672313/sniff-out-user-credentials-at-wi-fi-hotspots-with-firesheep [Accessed September 2014].

[52] Bott, E, (2013), "Do you save passwords in Chrome? Maybe you should reconsider", *ZNET*, Available at: http://www.zdnet.com/do-you-save-passwords-in-chrome-maybe-you-should-reconsider-7000019074/ [Accessed September 2014].

[53] Baskin, B., Bradley, T., Faircloth, J., Schiller, C., Caruso, K., Piccard, P., James, L., Piltzecker, T. (2006), *Combating Spyware in the Enterprise*, Syngress Publishing.

[54] Zeltser, L., (2011),"How antivirus software works: Virus detection techniques", *Security Search*, Available at: http://searchsecurity.techtarget.com/tip/How-antivirus-software-works-Virus-detection-techniques [Accessed September 2014].

[55] Cuadra, F. (2003), *How an Antivirus Program Works*, Panda Software.

[56] Miretskiy, Y., Das, A., Wright, C., Zadok, E., (2004), *Avfs: An On-Access Anti-Virus File System*, USENIX.

[57] AntivirusWorld (n.d), How does anti-virus software work?,*AntivirusWorld*, Available at: http://www.antivirusworld.com/articles/antivirus.php [Accessed September 2014].

[58] AV-comparative, (2014), *Proactive Test: Heuristic and behavioural protection against new/unknown malicious software*, AV-Comparatives

[59] AV-comparative, (2014), *File Detection Test of Malicious Software*, AV-Comparatives

[60] MAAWG, APWG, (2006), *Anti-Phishing Best Practices for ISPs and mailbox providers*, MAAWG & APWG

[61] O'Brien, C., Vogel, C. (2004), *Spam Filters: Bayes V Hi-Squared*, Trinity College.

[62] Clark, K, (2008), A Survey of Content-based Spam Classifiers, Available at: http://www.iids.org/aigaion/indexempty.php?page=actionattachment&action=open&pub_id=328&location=clark2008scb.pdf-ed2fb41e85a7718e8d1d1ae44432e458.pdf [Accessed September 2014].

[63] Gregg, T, Roshan, T, Tom, V (2004), *Anti-Phishing: Best Practices for Institutions and Consumers*, McAfee

[64] Kumaraguru P, Cranshaw J, Acquisti A, Cranor L, Hong J, Blair M, Pham T, (2009), "School of Phish: A Real-World Evaluation of Anti-Phishing Training", *Symposium on Usable Privacy and Security (SOUPS) 2009*, July 15–17, 2009, Mountain View, CA USA

[65] Ferrara, J, (2009), *Security Officers and Users Find Common Ground Through Simulated Phishing Attacks*, Wombat Security

[66] Zhang, Y., Hong, J., Cranor, L., (2007), "CANTINA: A Content-Based Approach to Detecting Phishing Web Sites", 2007*Proceedings of the 16th international conference on World Wide Web*, New York, pp:639-648.

[67] Chen, K., Chen, J., Huang, C., Chen, C., (2009), "Fighting Phishing with Discriminative Keypoint Features of Webpages", *Academia Sinica Institute of Information Science*, Available at: http://www.iis.sinica.edu.tw/papers/song/10971-F.pdf [Accessed September 2014].

[68] Toolan, F., Carthy,J., (2009), "Phishing detection using classifier ensembles,"*eCrime Researchers Summit*, Oct 2009, pp. 1 –9.

[69] Cook, D., Gurbani, V., M. Daniluk, (2008), "Phishwish: A stateless phishing filter using minimal rules," *Financial Cryptography and Data Security*, Springer-VerlagBerlin, Heidelberg, 2008, pp. 182–186.

[70] Prakash, P., Kumar, M., Kompella, R., Gupta, M., (2010), "PhishNet: Predictive Blacklisting toDetect Phishing Attacks", *INFOCOM*,Available at: https://www.cs.purdue.edu/homes/kompella/

[71] publications/infocom10phishnet.pdf [Accessed September 2014].

[72] Yue, C., Wang, H.,(2010), "BogusBiter: A transparent protection against phishing attacks",*ACM Transactions on Internet Technologies*, May 2010, 10 (2).

[73] Knickerbocker, P., Yu, D., Li J., (2009), "Humboldt:A Distributed Phishing Disruption System", *eCrime Researchers Summit*, 2009, IEEE, pp: 1-12.

