Browser Blacklists: A utopia of phishing protection

Tsalis N. [1], Virvilis N. [1], Mylonas A. [2, 1], Apostolopoulos T. [1], Gritzalis D. [1]

[1] Information Security & Critical Infrastructure Protection Laboratory, Dept. of Informatics, Athens University of Economics & Business, 76 Patission Ave., GR-10434, Athens, Greece

[2] Faculty of Computing, Engineering and Sciences, Staffordshire University, Beaconside, ST18 0AD Stafford, United Kingdom

{ntsalis, nvir, amylonas, tca, dgrit}@aueb.gr,
alexios.mylonas@staff.ac.uk

Abstract. Mobile devices - especially smartphones - have gained widespread adoption in recent years, due to the plethora of features they offer. The use of such devices for web browsing, accessing email services and social networking is also getting continuously more popular. The same holds true for other more sensitive online activities, such as online shopping, contactless payments, and web banking. However, the security mechanisms available on smartphones are not yet mature, while their effectiveness is still questionable. As a result, smartphone users face increased risks when performing sensitive online activities with their devices, compared to desktop/laptop users. In this paper, we present an evaluation of the phishing protection mechanisms that are available with the popular web browsers of the Android and iOS platform. Following, we compare the protection they offer against their desktop counterparts, revealing and analyzing the significant gap between the two. Finally, we provide a comparison between the Safe Browsing API implementation in Google Chrome and the Safe Browsing Lookup API, revealing significant inconsistencies between the two mechanisms.

Keywords: Android, Chrome, iOS, Mobile, Phishing, Smartphone, Safe Browsing Lookup API, Security, Web Browser, Windows.

1 Introduction

The proliferation of smartphones is increasing. According to [2], in the Q3 of 2013 more than 445M mobile phones were sold, out of which 250M were smartphones. Despite the unarguably important benefits and capabilities which they offer, the use of such devices - especially for sensitive online tasks - has turned them into a new profitable target for both sophisticated, and less skilled attackers [3].

Nowadays: (a) smartphones are frequently used as part of a two-factor authentication scheme for online services (e.g. e-banking), (b) wireless payments using NFC-enabled smartphones are getting continuously more popular, exceeding 235B$ in 2013 [4], (c) the use of smartphones in business is also increasing (e.g. under the Bring Your Own Device (BYOD) trend), even in sensitive environments, with iOS and Android devices getting accredited for use in the US Dept. of Defense [5], and (d) smartphones have become appealing targets as recent reports have revealed [6].

One of the threats that target (smartphone) users is phishing. Phishing can be deemed as one of the most popular and profitable attacks, with almost 450,000 attacks in 2013 and estimated losses of over 5.9B$. NIST defines phishing [7] as: *"Phishing refers to use of deceptive computer-based means to trick individuals into disclosing sensitive personal information. Phishing attacks aid criminals in a wide range of illegal activities, including identity theft and fraud. They can also be used to install malware and attacker tools on a user's system."*

Although the majority of phishing attacks are widespread and focus on financial gain, targeted phishing attacks also exist. These attacks are widely known as spear-phishing and have been used in a large number of sophisticated attacks against government, military and financial institutions. The analysis of past major security incidents, involving Advanced Persistent Threats (APT) [8], [9], has revealed that attackers used targeted phishing attacks in order to gain access to the internal network of their target.

In this paper, we evaluate the protection offered against phishing attacks on smartphone platforms. The scope of our analysis includes the popular browsers in Android and iOS. We measured the protection offered by these browsers, by accessing more than 5,000 manually verified phishing URLs, within a period of two months. We performed the same evaluation against popular desktop browsers and compared their detection rate. Our results indicate a significant gap in the effectiveness of phishing protection between smartphone and desktop browsers. Thus, we collected and analyzed all the URLs of phishing campaigns that have not been filtered out by the browsers in any of the two platforms, so as to identify the common characteristics that enable us to strengthen our defenses against the above threat.

In addition, we evaluated the phishing protection provided by the Safe Browsing API (as implemented in Google Chrome) and the Safe Browsing Lookup API. Finally, we expanded our research regarding phishing campaigns and derived statistics for the period between Jan-Dec 2014, identifying the most targeted web sites and services.

This paper makes the following contributions: (a). It provides a comparison of the phishing protection offered by popular browsers in Android, iOS and Windows platforms, (b). It provides a comparison between Google's Chrome browser and the Safe browsing Lookup API with regards to phishing protection, highlighting discrepancies when different API's are used to query the Safe Browsing list, and (c). It presents an analysis of successful phishing campaigns and proposes countermeasures that can be used to strengthen our defenses against phishing.

The remainder of the paper is structured as follows: Section "Background" presents related work. Section "Methodology" describes the methodology used for the experiments conducted. Section “Results” presents the comparison between mobile browsers and their desktop counterparts, Section “Safe browsing API” focuses on the effectiveness of the Safe Browsing list by comparing two different query API’s, while Section “Phishing campaigns” presents phishing campaign statistics. The paper ends with conclusions and suggestions for further work in Section “Conclusions and future work”.

2 Background

The main defense against phishing attacks is based on lists (i.e. 'blacklists'), which are used by browsers to identify if a requested URL must be blocked or not. Such a prominent blacklist is Google’s Safe Browsing [10], which protects users both from phishing and malware web sites. Safe Browsing is currently used by Google Chrome, Mozilla Firefox and Apple Safari browsers. Internet Explorer is using Microsoft’s proprietary blacklist, the SmartScreen [11]. Other browsers also use their own proprietary lists, as well as aggregate information from third parties. For instance, Opera uses a combination of blacklists from Netcraft [12] and PhishTank [13], as well as a malware blacklist from TRUSTe [14].

Although each blacklist implementation is different, all of them follow a basic concept, i.e., before a URL is loaded by the browser, a URL check occurs via data from a local or remote database. If the current URL matches a known malicious site, a warning is raised to the user advising her to avoid browsing to the current URL. Limited information is available on how these blacklists get updated and maintained, as this could enable attackers to bypass them more easily. However, a considerable part of the submissions to blacklist are performed manually by users [13].

Based on the number of the submissions to anti-phishing sites, such as PhishTank, it turns out that phishers are very active, generating several hundred phishing pages/domains on a daily basis. The main reason for the popularity of such attacks, regardless of the attackers objective (e.g. identity theft, malware infection, information gathering, etc.), is their effectiveness. The use of blacklists always allows a window of several hours when attackers can exploit their victims [14]. To make the matters worse, our work shows that this window is significantly larger on mobile devices (i.e. Safari Mobile) due to the way blacklists are getting updated.

The academic literature has also focused on combating this threat. As a result, a number of approaches have been proposed in an effort to protect the users from phishing attacks. This research varies from surveys regarding user awareness, to experiments of the effectiveness of current security mechanisms and proposals of novel ones. More specifically, the work in [15], [16] and [17] focuses on phishing with regards to its properties, characteristics, attack types, and available countermeasures. Also, [17] and [18] present a survey on user training methods, as well as their effectiveness against phishing attacks, as user participation plays a major role in phishing protection.

Literature has also focused on the use of visual indicators to protect users from phishing. In [19] an overview of the warning indicators and its advances over the last decade is presented. Also, [20] has surveyed users' interaction with security indicators in web browsers. A study on the effectiveness of browser security warnings was published in [21], focusing on the Google Chrome and Mozilla Firefox browsers. The authors collected over 25M user reactions with phishing and malware security warnings, measuring the user reactions to these warnings. A similar study [22] analyzed the impact on the users' decision based on the choice of background color in the warning and the text descriptions that were presented to them. In [23], the authors conducted a survey regarding the effectiveness of security indicators, comparing the warning messages of Firefox and Internet Explorer.

In [24], the authors focused on the effectiveness of phishing blacklists, in particular on their update speed and coverage. The authors used 191 phishing sites that had been active for 30 min or less, and compared 8 anti-phishing toolbars. Less than 20% of the phishing sites were detected at the beginning of the test. In addition, they identified that blacklists were updated in different speeds, which varied from 47-83%, 12 hours after the initial test. Similarly in [25], the authors proposed the use of 'Anti-Phish', a browser extension for the Mozilla Firefox browser, so as to detect web site-based phishing attacks.

A Novel-Bayesian classification, based on textual and visual content, was proposed in [26]. Authors used a text classifier, an image classifier, and a fusion algorithm to defend against known properties of phishing attacks. Furthermore, [16] provides a methodology that aims to distinguish malicious and benign web pages, which is based on layout similarity between malicious and benign web pages.

In [27], the authors analyzed 300 phishing URL and measured the effectiveness of desktop browsers in detecting them. Opera browser offered the highest level of protection, by blocking 94.2% of the phishing sites. In [28], the authors tested the effectiveness of anti-phishing add-ons for Internet Explorer, Google Chrome and Mozilla Firefox. In their evaluation Google Chrome outscored the other browsers. Finally, in [12] authors tested popular desktop web browsers (i.e. Firefox, Chrome, Opera, IE, Safari), focusing on the time required for browsers to block a malicious site. The initial results (zero-day) ranged from 73.3% (IE) to 93.4% (Safari), while the final results (7-day) varied from 89.3% (IE) to 96.6% (Firefox).

A number of anti-phishing mechanisms have been proposed for use in smartphones. In [29], the authors investigate the viability of QR-code-initiated phishing attacks (i.e. QRishing) by conducting two separate experiments. A similar approach was presented in [30], where authors worked on how notification customization may allow an installed Trojan application to launch phishing attacks or anonymously post spam messages.

Related work on browser security revealed that security controls that are typically found on desktop browsers are not provided in their smartphone counterparts [31]. In our work we also find that smartphone browsers still do not offer anti-phishing protection. Moreover, the analysis in the same work, revealed that the implementation of the security controls (among them the security control against phishing attacks) was not hindered by restrictions from the security architecture (i.e. the application sandbox). The related literature does not adequately focus on the effectiveness of anti-phishing mechanisms on Android and iOS browsers.

3 Methodology

The scope of our work includes popular desktop browsers, i.e. Chrome, Internet Explorer, Firefox, and Opera, together with their smartphone counterparts. In smartphones, the scope of our analysis focuses in iOS and Android, as they are the prominent smartphone platforms, having ~90% of the global market share [32].

For the evaluation of smartphone browsers, an iPhone 5S was used for iOS, and a Sony Xperia Tipo for Android. Browser availability in the two smartphone platforms is heterogeneous, meaning that not all browsers are available in both platforms (see Table 1).

To evaluate the protection that is offered by the above mentioned web browsers, we visited phishing URL that were indexed in PhishTank. We selected phishing URL that were confirmed - i.e. PhishTank confirmed the reported URL as a fraudulent one - and online. However, the state of a phishing URL is dynamic, namely a confirmed URL might be cleaned or be taken down short after its submission to an anti-phishing blacklist list. Therefore, all the URL were manually examined to separate web pages that have been cleaned (i.e. false positives) from the ones that were fraudulent and not filtered out by the browsers' blacklists (i.e. false negatives).

Table 1. Browser availability

	iOS 7.0.4	**Android 4.0.4** (Sony Xperia Tipo)	**Windows 7** (64bit)
Safari Mobile	X		
Chrome Mobile	X	X	
Opera Mini	X	X	
Browser[†]		X	
Firefox Mobile		X	
Opera Mobile		X	
Chrome			X
Firefox			X
Internet Explorer			X
Opera			X

[†] 'Browser' is the pre-installed browser in Android

We collected URL from PhishTank for 2 months (Jan-Mar 2014). During this period we noticed that their number fluctuated significantly, with an average of several hundred URL per day. Although some of the evaluation could be automated (e.g. URL that returned HTTP Error Codes or URL for which the browsers raised warnings), it was necessary to verify whether URL, that were not filtered-out by the browsers as fraudulent, were actually legitimate sites (i.e. not false negatives). This required manual verification. To keep the analysis manageable, each day we manually verified at most 100 URL, which were indexed in PhishTank as confirmed and online. In case, more than 100 URL were submitted to PhishTank on a given day, we randomly selected 100 of them.

In total, we collected and evaluated the web browsers that were in our scope, against 5651 phishing sites. Each URL was categorized into one of the following categories:

1. *Blacklisted:* The URL was filtered-out by the web browser, i.e. the user receives a warning indicating the threat of a potential phishing site.
2. *False Negative:* Denoting a phishing site that was manually verified by us as fraudulent, but was not on the browser's blacklist (e.g. the browser generated no warning).
3. *Non-Phishing/Timeout/Error:* A site that during our manual verification had either been cleaned, or suspended/taken down when we accessed it.

For each URL found to be a false negative, we kept the URL and the contents of the malicious phishing page. This enabled us to identify the most popular phishing targets, as well as identify patterns that helped us improve the detection mechanisms.

Finally, for each URL that was collected, we used the Safe Browsing Lookup API [8] to query directly the Safe Browsing database. This enabled us, to compare the results from the Safe Browsing Lookup API with the web browsers' results.

Table 2. Support of anti-phishing mechanisms

Platform	Browser name	Phishing protection[†]
iOS	Safari Mobile	Y
	Chrome Mobile	N
	Opera Mini	N
Android	Browser[††]	N
	Firefox Mobile	Y
	Chrome Mobile	N
	Opera Mobile	Y
	Opera Mini	N
Windows 7	Firefox	Y
	Chrome	Y
	Opera	Y
	Internet Explorer	Y

[†] Y: Security control available, N: Security control not available
[††] 'Browser is the pre-installed browser in Android

4 Results

4.1 Overview

A finding that arose early in our analysis is that only a subset of the mobile browsers supported anti-phishing protection (see Table 2). Thus, their respective users were unprotected from phishing attacks. On the contrary, all desktop browsers provided anti-phishing protection, even though their effectiveness differed significantly. Table

2 summarizes the availability of anti-phishing protection per operating system and browser (as of March 2014).

The results of our analysis are presented in Figs. 1-3. More specifically, (a) Fig. 1 presents the percentage of blocked URL per browser, (b) Fig. 2 depicts the percentage of active phishing URL that were not filtered out, namely the ones that were not in the browser's blacklist and were manually verified as active malicious sites (false negatives), and (c) Fig. 3 presents the percentage of URL that were not in the browser's blacklist and were manually verified during our analysis as non-malicious sites (i.e. URL that had been cleaned, or domains that had been taken down or were not accessible when we accessed them). The browsers that did not support any anti-phishing mechanism are not included in the charts, as their detection rate is zero.

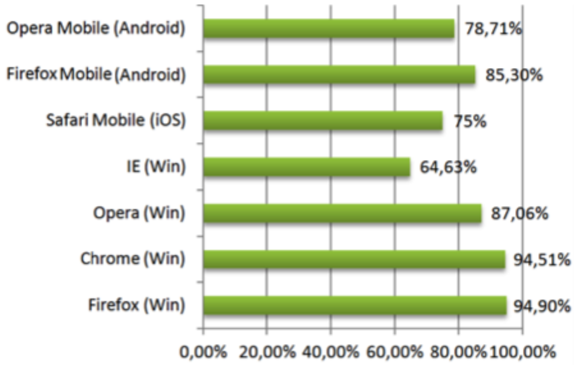


Fig. 1. Percentage of blocked URLs (n=5651)

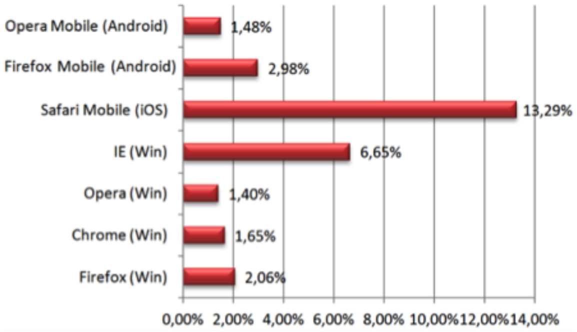


Fig. 2. Percentage of phishing URLs that were not filtered out (n=5651)

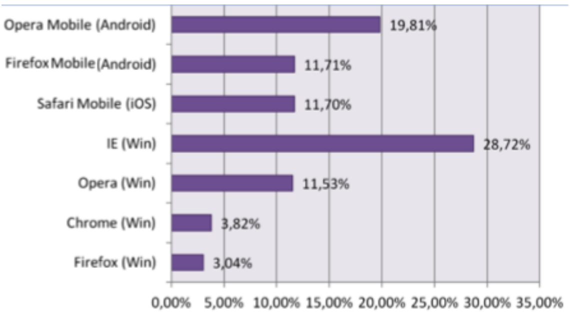


Fig. 3. URLs not in blacklist and not phishing (manual verification, n=5651)

For further information, the detailed results (per browser) are depicted in Table 3.

Table 3. Detailed results per browser

Browser	Black-listed	False negatives	Non-phishing
Safari Mobile (iOS)	4239	751	661
Firefox Mobile (Android)	4821	168	662
Opera Mobile (Android)	4448	84	1119
Firefox (Windows)	5362	117	172
Chrome (Windows)	5341	94	216
Opera (Windows)	4920	79	652
IE (Windows)	3653	376	1622

4.2 iOS browsers

In iOS devices, Mobile Safari - which is the default (i.e. pre-installed) web browser of the platform - supports the detection of fraudulent websites by utilizing Google's Safe Browsing blacklist. Our evaluation revealed that the anti-phishing control suffers from a significant design weakness. This holds true since the Safe Browsing blacklist is only updated when a user synchronizes her iOS device with iTunes (on a desktop/laptop). Considering that a subset of iOS users may not synchronize their devices frequently (e.g. when they are on a trip) or at all, they end up with an outdated blacklist. Thus, these users eventually receive only a limited protection against phishing attacks.

Our analysis also revealed that (see Fig. 1-3): (a) Mobile Safari had significantly more false negatives (i.e. phishing URL that were not filtered out) comparing to the other mobile web browsers, and (b) iOS users can be protected from phishing attacks only when they use Mobile Safari, since Opera Mini does not offer such protection. Chrome Mobile on iOS offers phishing protection since January 2014, however, this functionality is disabled by default. It requires the user to enable the "Reduce Data Usage" option, which uses Google's servers to fetch the requested web pages (URL and contents). This feature is privacy intrusive (as all traffic is transferred through Google's Server), does not work for SSL/TLS pages or in private browsing mode. We have excluded it from our evaluation as: a) we regard that it is less likely that ordinary users (i.e. not security and savvy ones) will enable security controls, as smartphone users tend to be oblivious about their security and privacy [33] and (b) the control is not 'easily configurable' [34], i.e., the label of the control is not intuitive, thus confusing even security savvy users that control focuses on performance and not security.

4.3 Android browser

In Android, the default web browser (commonly known to Android users as "Browser" or "Internet") offers no phishing protection. The same applies to the Mobile Chrome and Opera Mini browsers. Our evaluation revealed that Android users can only be protected from phishing attacks if they use Firefox Mobile and Opera Mobile. Also, our results revealed that the two above mentioned browsers offer comparable but not equal protection from phishing with their desktop counterparts.

If one considers that: (a) not all users are willing and/or capable to install a third party browser on their devices and (b) the pre-installed browser offers no protection, then a very large number of Android users are not adequately protected from phishing attacks.

4.4 Desktop browser

All desktop web browsers offered phishing protection using either Google's Safe Browsing (i.e. Chrome and Firefox) or their own proprietary blacklists (i.e. in Opera and Internet Explorer). The protection against phishing in Chrome and Firefox was similar; both blocked almost all the fraudulent URL that we tested. At the same time, they achieved low false negatives. However, this similarity in their performance was expected, as both use the same blacklist.

During our experiments we found another issue with the synchronization of blacklists, which offers a window of exploitation to phishers. We noticed that if the desktop browsers were not executing for a few minutes before we started our evaluation, then the blacklist was not updated. This is especially true for Firefox, as in this web browser we frequently encountered a large number of false negatives (i.e. phishing pages that were not blocked) during the first few minutes of our tests. This is very likely due to the way that the Safe Browsing protocol updates the list of malicious sites [35]. Interestingly enough we did not face this problem in Chrome. In [14], authors highlighted the same issue during their tests for an older version of Chrome, which adds to our suspicion that the inconsistent results are due to the Safe Browsing protocol's update procedure.

As summarized in Figs. 1-3, Opera outscored in our evaluation the rest browsers. Even though the percentage of blocked URL was less, this does not translate to a less accurate blacklist. This holds true, as the percentage of false negatives (i.e. the phishing sites that were not filtered out) is lower than both Chrome and Firefox. As a matter of fact, it seems that Opera's blacklist is updated more frequently, as it did not block URL that had been cleaned or taken down, while these URL were still blocked by the browsers that used the Safe Browsing blacklist.

Finally, the proprietary blacklist that Internet Explorer uses, i.e. Microsoft's SmartScreen, offered the least protection in the desktop browsers. As our results indicate, Internet Explorer had the highest rate of false negatives among them, i.e. filtered out fewer manually confirmed phishing URL than the other desktop web browsers.

5 Safe browsing API

For each test URL of our analysis, we used Google’s Lookup API [35] to query directly the Safe Browsing blacklist, to compare its results with the browsers' results. The results from the Safe Browsing Lookup API differed significantly from those of Chrome and Firefox browsers. More specifically, on average only 73.21% of the URL that were blocked by Chrome and Firefox, were reported as malicious by Google’s Safe Browsing Lookup API. After manually verifying the URL that were not blocked, we noticed that their majority were active phishing sites (i.e. false negatives of the API).

Two ways are available for querying the Safe Browsing database: (a) using the Safe Browsing API, or (b) using the Safe Browsing Lookup API [10]. The first, which is used by web browsers, offers better privacy as the browser does not need to send the queried URL to Google for analysis; also, it is optimized for a large number of requests. The latter offers simpler implementation (i.e. a single HTTP GET request) and can be used for testing up to 10.000 URL per day. Nevertheless, both API query the same database according to Google [10] and should provide the same results.

Our initial experiments revealed that the results between these two ways differ significantly.

As this is an interesting finding, we repeated the tests in December 2014, with a new data set and compared once more the results from the two APIs. More specifically we compared the results of Google’s Chrome (v. 39.0.2171.71 m) browser (latest at the time of this writing) and the results of Safe Browsing API, by accessing 100 URL’s per day, for 10 continuous days. The results are shown in the following table.

Similarly to our initial results Google Chrome using Safe Browsing API blocks significantly more (19.1%) phishing URLs compared to the results of Safe Browsing Lookup API. The reason for this discrepancy is unclear. This may be due to the fact that: (a) web browsers use additional anti-phishing mechanisms which complement the Safe Browsing list and/or (b) the Safe Browsing API and Safe Browsing Lookup API do not query the same data set, contrary to Google’s documentation [10].

Table 4. API Comparison

Date	**Blacklisted** (Safe Browsing API) n=1000	**Blacklisted** (Safe Browsing Lookup API) n=1000
3/12/14	98	87
4/12/14	96	86
5/12/14	91	76
6/12/14	94	72
7/12/14	91	58
8/12/14	100	79
9/12/14	85	73
10/12/14	83	63
11/12/14	88	62
12/12/14	99	78
Total	**925**	**734**
Percentage	**92.5%**	**73.4%**

6 Phishing campaigns

6.1 Phishing campaigns' statistics

During our experiments we noted every phishing campaign (both URL and page contents) that was manually verified as phishing, but was not filtered out by at least one of the web browsers in our scope that supported anti-phishing protection. The analysis of the phishing URL that were not filtered out aimed at identifying the most popular phishing targets. It also aimed at highlighting similarities between phishing campaigns that could be used to strengthen our defenses against such attacks. Table 5 summarizes these results.

Table 5. Main phishing campaigns

Target	Percentage	String in URL
paypal.com	61.68%	48.19%
appleid.apple.com	15.17%	47.61%
Banks (Multiple)	4.41%	N/A
Web Email (Multiple)	5.10%	N/A
Random Campaigns	13.64%	N/A

PayPal was the primary target of the phishing campaigns, as 61.68% of the phishing URL that were tested targeted PayPal users.

The second most popular target was Apple, with 15.17% of the phishing URL targeting Apple users. A compromised Apple account gives access to all information stored on the victim's iCloud account [36], including contacts, calendar, email, files and photos. Therefore, this is another fruitful target for attackers.

The rest of the phishing results have been divided in three generic categories:

1. *Banks* - Phishing campaigns that target online banking from various banks.
2. *Email* - Phishing campaigns that target web based email providers (Gmail, Yahoo Mail, Outlook).
3. *Misc* - Random phishing campaigns against other websites.

Our analysis revealed that in the two popular phishing campaigns, the 48.19% and 47.61% of them contained in their URL the word "paypal" or "apple", respectively. By including those strings in the URL (preferably in the beginning), the phishing attack is more likely to succeed against naive users who do not inspect the URL.

Our results suggest that web browsers can implement URL filtering based on regular expressions, so as to increase their detection rate against sites that are not yet blacklisted. For instance, web browsers can change the color of the location bar or issue a warning to the user, when visiting a URL that includes the string of a popular site (e.g. "paypal", Table 6), while the URL does not originate from a benign web site (e.g. www.paypal.com or www.paypalobjects.com). Such a solution might not scale adequately for a large number of sites, but it could be implemented to protect a few hundred of popular ones, similar to Google Chrome's Certificate Pinning for specific sensitive domains [37]. Nevertheless, such countermeasures can only partially address the problem. Only a multi-layered defense of both technical and procedural means, will enable us to defend effectively against the phishing threat [38], [39].

Table 6. Phishing URL

Target	**URL**[†]
Paypal	http://**paypal.com**.cgi-bin-websc5.b4d80a13c0a2116480.ee0r-cmd-login-submit-dispatch-5885d80a13c0d.b1f8e26366.3d3fae.e89703d295b4.a2116480e.e013d.2d8494db97095.b4d80a13c0a2116480.ee01a0.5c536656g7e8z9.real.domain.name.removed?cmd=_home&dispatch=5885d80a13c0db1f8e&ee=8ae65ec5a442891deac1bc0534a61adb
	http://**paypal.com**.*real.domain.name.removed*/update/?cmd=_home&dispatch=5885d80a13c0db1f8e&ee=46accb06788060b6e5ae1a1a964d625c

[†] The domain names have been anonymized

6.2 Analysis of PhishTank's statistics

To further expand our research, we visited PhishTank and derived statistics based on the published phishing database. More specifically, we collected the submitted phishing URL's from January to December 2014, which rounded up to 19826 URL's. Following, we identified the top 8 phishing campaigns and grouped them together when applicable: *Amazon*, *Apple Services*, *Ebay*, *Facebook*, *Financial Institutions(Banks)*, *Google Services* and *Paypal*. It should be noted that the categorization was based on the results published by Phishtank and there was no way to verify their validity, as the vast majority of the phishing sites were no longer accessible. Unfortunately only a small percentage of results were categorized by Phishtank and thus, the analysis was based on this limited data, ignoring any uncategorized URL (marked as

“Other” by Phishtank and in the table below). The following tables include the aforementioned elements, categorized both by month and target:

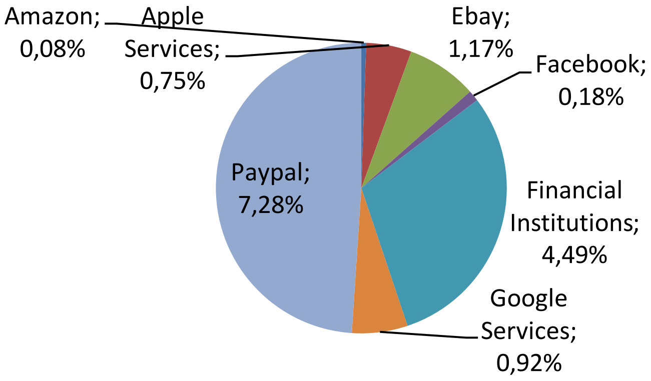
Table 7. PhishTank statistics per month

	Amazon	Apple Services	Ebay	Facebook	Financial Institutions	Google Services	Paypal	Other
January	0%	0.47%	0%	0%	1.89%	0.47%	5.19%	91.98%
February	0%	0.81%	1.22%	0%	14.23%	1.63%	8.13%	73.98%
March	0.20%	0.20%	1.19%	0%	30.04%	0.40%	4.35%	63.64%
April	0%	0%	0.09%	0%	29.22%	0.19%	3.04%	67.46%
May	0%	0%	0.90%	0%	17.51%	0.30%	3.59%	77.69%
June	0%	0.71%	0.71%	0.53%	3.91%	1.07%	3.91%	89.15%
July	0%	0.28%	1.97%	0.28%	2.53%	0.84%	8.43%	85.67%
August	0%	0.73%	1.61%	0.73%	3.22%	0.88%	9.81%	83.02%
September	0%	1.79%	1.62%	0.09%	3.33%	0.68%	6.74%	85.75%
October	0.16%	0.59%	1.89%	0.22%	2.16%	0.75%	4.80%	89.43%
November	0.02%	0.66%	1.42%	0.21%	1.36%	1.79%	4.27%	90.25%
December	0.14%	0.95%	0.91%	0.14%	1.24%	0.63%	10.77%	85.22%

Table 8. PhishTank statistics per category

Category	No of URL’s	Percentage
Amazon	16	0.08%
Apple Services	155	0.75%
Ebay	241	1.17%
Facebook	36	0.18%
Financial Institutions	922	4.49%
Google Services	188	0.92%
Paypal	1495	7.28%

Fig. 4. Main targets



Based on these statistics, the most popular phishing target was Paypal, with approximately 7.28% of the phishing URL’s targeting the service. Financial Institutions (banks) follow next with 4.49%. This confirms the fact that the prime target for phishers is monetary gain. Ebay follows with 1.17%. Last but not least, all the other targets (i.e. Amazon, Apple Services, Facebook and Google Services) hold less than 1% each, with the Amazon element to hit the lowest percentage, i.e. 0.08%.

Finally, similarly to what we had done with our initial data set (see section 6.1), we analyzed all classified URLs in the new data set. Our goal was once more, to identify whether for each targeted service/site, there was a corresponding string in the URL (i.e. if the target was paypal.com we search the URL for the string "paypal"). The following table presents the percentage of URLs which included the target's string somewhere in the URL. The results support our previous recommendation (see section 6.1) for performing additional checks on the URL as a means of detecting phishing campaigns.

Table 9. Main phishing campaigns revisited

Category	String in URL
Amazon	18.75%
Apple Services	32.90%
Ebay	46.89%
Facebook	19.44%
Financial Institutions	N/A
Google Services	23.94%
Paypal	40.64%

7 Conclusions and future work

Nowadays phishing is one of the most popular and profitable attacks. Our work reveals that Android and iOS users are not adequately - or sometimes not at all - protected from this threat.

More specifically, our work evaluates the anti-phishing protection that is offered by web browsers within a period of two months, against several thousand phishing URL. The scope of our analysis includes popular browsers in iOS, Android and Windows platforms. Our results revealed that only a subset of browsers in iOS and Android offer potentially adequate phishing protection, leaving their users exposed to such attacks. For instance, in Chrome Mobile and Opera Mini do not offer anti-phishing mechanisms. In Android, which is currently the most popular smartphone platform, the pre-installed browser (i.e. "Browser" or "Internet") does not offer anti-phishing protection. Therefore, Android users who are not using a third-party browser that offers such protection, are exposed to phishing attacks.

Our results also point out that the anti-phishing protection that is offered by the mobile browsers is not as effective as in their desktop counterparts. This is true in cases where the same blacklist is used (e.g. in Safari Mobile that uses the Safe Browsing blacklist), and/or the same browser in different platform (e.g. Opera Mobile and Opera for desktop, Firefox Mobile and Firefox for desktop).

To make the matters even worse, our analysis has revealed implementation/design flaws that limit the effectiveness of blacklists. For instance, we discovered that Mobile Safari (i.e. the pre-installed browser in iOS) requires a synchronization with iTunes so as to download the latest version of Safe Browsing list. Thus, if users fail to synchronize their devices they will not be alerted when accessing known phishing sites. Moreover, it is more likely that iOS users are unaware that failing to synchronize their device with iTunes lowers their security while they browse the web.

In desktop browsers, despite the fact that the popular web browsers included anti-phishing mechanisms, their effectiveness varied significantly. Internet Explorer offers the least protection from phishing attacks, while Opera offers the highest level of protection. Firefox and Chrome offered similar level of protection.

In addition, our results revealed discrepancies between the Safe Browsing API and Safe Browsing Lookup API, which has a number of security implications.

Regarding phishing campaigns, our statistics revealed that the main goal for phishers is financial gain, something which was expected (i.e. targeting Paypal and Financial Institutions).

The above mentioned findings are very worrisome if one considers the proliferation of mobile devices. We thus suggest that all vendors of mobile browsers need to implement protection mechanisms at least as efficient as the ones offered by the desktop browsers. In the mean-time, users of mobile devices should use third-party web browsers that offer phishing protection and/or on web filtering proxies.

As future research, we plan to further test the effectiveness of phishing blacklists that are provided by mobile browsers. We also plan to investigate and implement additional countermeasures that can be used to combat phishing.

References

1. Virvilis N., Tsalis N., Mylonas A., Gritzalis D.: Mobile devices: A phisher's paradise. In: 11th International Conference on Security and Cryptography (SECRYPT-2014), pp. 79-87, ScitePress, Austria (2014)
2. Gartner: Gartner Says Smartphone Sales Accounted for 55 Percent of Overall Mobile Phone Sales in 3rd Quarter of 2013, https://www.gartner.com/newsroom/id/2623415
3. Mylonas A., Dritsas S, Tsoumas V., Gritzalis D.: Smartphone Security Evaluation - The Malware Attack Case. In: 8th International Conference on Security and Cryptography, pp. 25-36, SciTePress, Spain, July (2011)
4. Gartner: Gartner Says Worldwide Mobile Payment Transaction Value to Surpass $235 Billion in 2013, https://www.gartner.com/newsroom/id/2504915
5. Capaccio, N.: Apple Mobile Devices Cleared for Use on U.S. Military Networks, http://www.bloomberg.com/news/2013-05-17/apple-mobile-devices-cleared-for-use-on-u-s-military-networks.html
6. CBC: Smartphones becoming prime target for criminal hackers, http://www.cbc.ca/news/technology/smartphones-becoming-prime-target-for-criminal-hackers-1.2561126
7. Mell, P., Kent, K., Nusbaum, J.: Guide to malware incident prevention and handling, National Institute of Standards and Technology (NIST), (2005)

8. Virvilis N., Gritzalis D.: Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?. In: 10th IEEE International Conference on Autonomic and Trusted Computing, pp. 396-403, IEEE Press, Italy (2013)
9. Virvilis N., Gritzalis D.: The Big Four - What we did wrong in Advanced Persistent Threat detection?. In: 8th International Conference on Availability, Reliability and Security, pp. 248-254, IEEE, Germany (2013)
10. Google: Safe Browsing API, https://developers.google.com/safe-browsing/
11. Microsoft: SmartScreen Filter, http://windows.microsoft.com/en-us/internet-explorer/products/ie-9/features/smartscreen-filter
12. Netcraft: Phishing Site Feed, http://www.netcraft.com/anti-phishing/phishing-site-feed/
13. PhishTank: Join the fight against phishing, https://www.phishtank.com/
14. Abrams R., Barrera O., and Pathak J.: Browser Security Comparative Analysis, NSS Labs, 2013, https://www.nsslabs.com/reports/browser-security-comparative-analysis-phishing-protection
15. Banu, M. Nazreen, S., Munawara Banu: A Comprehensive Study of Phishing Attacks. In: International Journal of Computer Science and Information Technologies, vol. 4, issue 6, pp. 783-786 (2013)
16. Rosiello, A. P., Kirda, E., Kruegel, C., Ferrandi, F.: A layout-similarity-based approach for detecting phishing pages. In: Security and Privacy in Communications Networks Workshops, pp. 454-463 (2007)
17. Rani, S., Dubey, J.: A Survey on Phishing Attacks. In: International Journal of Computer Applications, vol. 88, issue 10 (2014)
18. Jansson, K., Von Solms, R.: Phishing for phishing awareness. In: Behavior & Information Technology Conference, vol. 32, issue 6, pp. 584-593 (2013)
19. Bian R. M.: Alice in Battlefield: An Evaluation of the Effectiveness of Various UI Phishing Warnings, https://www.cs.auckland.ac.nz/courses/compsci725s2c/archive/termpapers/725mbian13.pdf
20. Darwish A., Bataineh E.: Eye tracking analysis of browser security indicators. In: Computer Systems and Industrial Informatics Conference, pp. 1–6 (2012)
21. Akhawe D., Felt A. P.: Alice in Warningland: A large-scale field study of browser security warning effectiveness. In: 22nd USENIX Security Symposium (2013)
22. Egelman S., Schechter S.: The Importance of Being Earnest [In Security Warnings]. In: Financial Cryptography and Data Security, Springer, pp. 52–59 (2013)
23. Egelman S., Cranor L., Hong J.: You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In: SIGCHI Conference on Human Factors in Computing Systems, pp. 1065–1074 (2008)
24. Sheng S., Wardman B., Warner G., Cranor L. Hong J., Zhang C.: An empirical analysis of phishing blacklists. In: 6th Conference on Email and Anti-Spam (2009)
25. Kirda E., Kruegel C.: Protecting users against phishing attacks with antiphish. In: Computer Software and Applications Conference, vol. 1, pp. 517–524 (2005)
26. Zhang, H., Liu, G., Chow, T. W., Liu, W.: Textual and visual content-based anti-phishing: A Bayesian approach. In: IEEE Transactions on Neural Networks, vol. 22, issue 10, pp. 1532-1546 (2011)

27. AV Comparatives: Anti-Phishing protection of popular web browsers. AV Comparatives, Dec 2012, http://www.av-comparatives.org/images/docs/avc_phi_browser_201212_en.pdf
28. Mazher N., Ashraf I., Altaf A.: Which web browser work best for detecting phishing. In: Information and Communication Technologies Conference, pp. 1–5 (2013)
29. Vidas T., Owusu E., Wang S., Zeng C., Cranor L., Christin N.: QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks. In: Financial Cryptography and Data Security, pp. 52–69 (2013)
30. Xu Z., Zhu S.: Abusing Notification Services on Smartphones for Phishing and Spamming. In: 6th USENIX conference on Offensive Technologies, pp. 1–11 (2012)
31. Mylonas A., Tsalis N., Gritzalis D.: Evaluating the manageability of web browsers controls. In: 9th International Workshop on Security and Trust Management, pp. 82-98, Springer (LNCS 8203), UK (2013)
32. Bradley, T.: Android Dominates Market Share, But Apple Makes All The Money, http://www.forbes.com/sites/tonybradley/2013/11/15/android-dominates-market-share-but-apple-makes-all-the-money/
33. Mylonas A., Kastania A., Gritzalis D.: Delegate the smartphone user? Security awareness in smartphone platforms. In: Computers & Security, Vol. 34, pp. 47-66, (2013)
34. Mylonas A., Gritzalis D., Tsoumas B., Apostolopoulos T.: A qualitative metrics vector for the awareness of smartphone security users. In: 10th International Conference on Trust, Privacy & Security in Digital Business (TRUSTBUS-2013), pp. 173-184, Springer (LNCS 8058), Czech Republic (2013)
35. Sobrier J.: Google Safe Browsing v2 API: Implementation notes, http://www.zscaler.com/research/Google%20Safe%20Browsing%20v2%20API.pdf
36. iCloud, https://www.icloud.com/
37. OWASP: Certificate and Public Key Pinning, https://www.owasp.org/index.Php/Certificate_and_Public_Key_Pinning
38. Theoharidou M., Kotzanikolaou P., Gritzalis D.: A multi-layer Criticality Assessment methodology based on interdependencies. In: Computers & Security, Vol. 29, No. 6, pp. 643-658 (2010)
39. Theoharidou M., Kotzanikolaou P., Gritzalis D.: Risk-based Criticality Analysis. In: 3rd IFIP International Conference on Critical Infrastructure Protection, Springer, USA (2009)