Security Threats of URL Shortening: A User's Perspective

Nhien-An Le-Khac and M. Tahar Kechadi

***Abstract*—Short URLs have been used on the Internet for several years now and as time goes by new security threats are discovered in relation to their use (e.g. malware, phishing, spam). However, although current research in literature has compiled addressing the security threats when utilizing such types of URLs, no study approached the assessment of user confidence and user awareness regarding short URLs. Thus the aim of this paper is to cover the existing knowledge gap and to compile a baseline assessment on the frequency of use, user confidence and user awareness when utilizing short URLs. To do so, we have developed questionnaire connected to the previously mentioned aspects and which was applied to one hundred persons of various nationalities from within the European Union with various user experiences when it comes to the Internet and short URLs. The analysis of the replies received from the participants to the survey has revealed a general awareness that there are security risks associated with short URLs, a tendency of propagation of short URLs to other Internet services and platforms.**

***Index Terms*—Security, threats, URL shortening, user perspective.**

I. Introduction

In a society where the Internet is used more and more in our daily lives, there is a need for the information to be delivered faster and without restraints. Information on the Internet is usually included in web pages, multimedia platforms, blogs, social networking sites that are all accessible via specific Uniform Resource Locator (URL). Currently some social networking sites as well as other websites pose certain limits as to the number of characters which a URL can include. Therefore, the need appeared for a service which would shorten a URL and deliver it to the user. The shortened URL would be just an alternative to the initial URL so that the user can access the same information without the restraint of the number of characters.

According to Wikipedia [1], "URL shortening is a technique on the World Wide Web in which a URL may be made substantially shorter in length and still direct to the required page. This is achieved by using an HTTP Redirect on a domain name that is short, which links to the web page that has a long URL. This is especially convenient for messaging technologies such as Twitter and Identi.ca that severely limit the number of characters that may be used in a message. Short URLs allow otherwise long web addresses to be referred to in a tweet". Another definition of the term short URL can also be found in [2]: "URL shortening services are used to replace a long "Internet Address" (URL) by a shorter one which usually does not exceed 30 characters. When users request the shortened URL, they are automatically redirected to the original URL."

Although the primary aim of URL shortening is to avoid the character limit set up by certain web services and platforms there are other uses for URL shortening such as to "beautify" a link, to track clicks or to disguise the underlying address. However, with this Internet service introduced, there appeared also ways to abuse it such as malware attacks (spam, malicious payloads etc.) that will also be detailed throughout the present paper.

Today, there are constantly new threats uncovered in relation to short URLs and new security risks identified for users. Yet, with all the focus on the risks in utilizing short URLs, no study approached the assessment of user confidence and user awareness regarding short URLs that in turn can prove effective in any cybercrime prevention policy or strategy.

The aim of this paper is to compile a baseline assessment on the user confidence and user awareness when utilizing short URLs following years of implementation of these services. This assessment may prove useful in developing user awareness products in relation to short URLs or cybercrime risks prevention material.

The rest of this paper organized as follows: Section II shows the related work of this research area. We present risks of using shortened URLs in Section III. We describe our adopted approach to evaluate the users' perspective on Security Threats of URL Shortening in Section IV. We show our experiments and analysis in Section V. Finally, we conclude and discuss on future work in Section VI.

II. Related Work

The topic of short URLs has been debated over a number of years as the security risks associated with their use poses significant concerns to users. Therefore the studies undertaken until present time have focused more on the risks implied by the use of short URLs rather than user confidence or user awareness regarding these shortened links.

In a joint study [3] presented during the Proceedings of the 2013 International World Wide Web Conference (WWW) by researchers from the Polytechnic University of Milan, Italy and the University of California, Santa Barbara, US, the risks of using short URLs were evaluated.

The study analyzed the measures taken by URL shortening services in preventing malicious links being shortened, focusing on spam, phishing and malware. The study also included an overview of the risks associated with the use of shortened URLs.

The research was based on the submission to URL shortening services of a specific number of URLs which

Manuscript received May 5, 2015; revised August 5, 2015.

The authors are with the School of Computer Science & Informatics, University College Dublin, Belfield, Dublin 4, Ireland (e-mail: an.lekhac@ucd.ie, tahar.kechadi@ucd.ie).

DOI: 10.7763/JACN.2015.V3.169

delivered exploits targeted at vulnerabilities in web browsers as well as browser plug- ins, URLs associated with phishing and URLs observed in spam e-mails with the purpose of determining whether URL shortening services block one or more classes of threats. According to the researchers, the results appeared to be consistent across the URL shortening services meaning that the services had implemented measures to detect malicious URLs such as blacklisting malicious domains from URL shortening and more real time monitoring of what URLs get shortened.

Although in some cases the shortening of malicious URLs was possible without restrictions, most of the URLs were flagged subsequently as malicious.

A study [4] compiled in May 2011 by researchers from the University of Aachen, Germany further detailed the security and privacy implications of URL shortening services. The study included an analysis of the security and privacy risks caused by the use of URL shortening services, an analysis regarding the malicious behavior, user tracking as well as leakage of URLs to search engines of the most popular URL shortening services used on Twitter and an analysis of the spam detection performance for the most popular URL shortening services. The study also included a new attack scenario to enable SSL-only circumvention using SSLStrip and shortened URLs. Following the research, the results yielded that none of the most popular URL shortening services at the time displayed any malicious behavior. However many of the shortening services were well-prepared for user tracking. Another outcome of the research was that by enumerating shortening services a significant amount of sensitive or private information could be found and that several shortening services leaked submitted URLs to search engines.

Another study compiled in March 2011 by researchers [5] from the Foundation for Research and Technology — Hellas, Greece provided a characterization on the usage of short URLs. The research was aimed at examining the content to which short URLs point to, how they were published, their popularity and activity over time as well as their potential impact on the performance of the web. Authors used in their study two sources of short URLs: collected from a large scale crawl of shortening services and collected by crawling Twitter messages. The outcome of the study was highlighted in several observations:

1) short URLs appear mostly in ephemeral media with profound effects on their popularity, lifetime and access patterns;
2) a small number of a very large number of hits while the majority of short URLs have very limited accesses;
3) short URLs become popular very fast which implies spikes in accessing of the links and corresponding traffic surges;
4) the most popular websites to which short URLs point to change slowly over time;
5) URL shortening services are extremely effective in space gaining, in more than 90% of the cases, the resulting short URL reduced the amount of bytes needed for the URL by 95%; however the imposed redirection of URL shortening services increased the web page access times by an additional 54%.

All the above studies introduce the risks associated with using short URLs and they assess the existing URL shortening services in terms of security of browsing on the Internet, measures taken by the administrators of URL shortening services, their popularity or existence over time. These studies have been presented since they are representative for the approach to focus on studies related to the risks of using short URLs.

However there is no individual study on the assessment of user confidence or user awareness associated with utilizing short URLs. Therefore, in our research, we aim to cover the gap on the user experience in relation to short URLs and to compile a baseline assessment on the frequency of use, user confidence and user awareness when utilizing short URLs. In this paper, we also include an overview on the risks associated to short URLs, which is instrumental in assessing the user experience in relation to shot URLs.

III. Risks of Using Shortened URLs

URL shortening services are popular when it comes down to shortening long URLs that have the possibility to break or are simply too long to be inserted in e-mails, posts on Social Networking websites or blogs. However the disadvantage is that with these URL shortening services you are no longer able to see directly where your browser will be pointed. Shortened URLs could lead to the following security risks:

1) sites which host malware, trojans and other malicious programs;
2) sites which could exploit security risks in a browser or system;
3) sites which contain phishing attempts and try to steal personal information;
4) sites which contain phishing attempts by social interaction;
5) sites which are being used in spam campaigns.

We discuss on these risks more details in the following sub-sections.

A. Spam

Spamming has become increasingly the most lucrative activity for hackers. URL shortening services are notorious [6] for being used by spammers in an attempt to avoid having their mail blocked by pointing at their own domains. They hope that by using a well-known, widely used, and free service that they will be able to avoid having their content filtered.

In a report [7] issued in May 2011 by Message Labs, evidence turned out that spammers established their own URL shortening services.

According to an article [8] from the examiner.com, following a spike in spamming by using the Google proprietary URL shortening service goo.gl, Facebook has started blocking the shortened URLs.

B. Malware

Previously malware associated domain names were easier to identify. The malware associated URLs tend to make less sense as it is difficult to obtain a domain name which looks similar to a legitimate site. Yet, with URL shortening services

you are using a well-known and "safe" domain. The possibilities are limited for most services to allow users to see the destination URL that a shortened URL points to.

For Facebook and Twitter, URL shortening services are common and users don't have second thoughts usually in accessing them. E-mail has become a less reliable means for phishing because of the anti-spam services involved. With URL shortening, it becomes easier because it "looks legitimate". It's a little more than an accepted form of obfuscation.

An example of URL shortening abuse was presented on the MX Lab Blog [9].

C. Phishing

According to the Global Phishing Survey [10] of semester two 2013, phishers continue to use “URL shortening” services to obfuscate phishing URLs. Users of those services can obtain a very short URL to put in their limited space posts, which automatically redirects the visitor to a much longer “hidden” URL. In the last report Global Phishing Survey, such use plummeted to only 270 attacks in the first semester of 2013, sharply down from 785 in the second semester of 2012. Unfortunately, the phishers have come back to using this technique again, with 999 such phishing attacks detected in the second semester of 2013.

IV. Adopted Approach

In order to evaluate the user perspective in relation to short URLs, a survey was conducted aimed at creating a baseline assessment of the most frequent use of shortened URLs, user confidence and user awareness on the risks associated.

The Survey Questionnaire was conceived based on the "intelligence led policing" approach, in the sense that in the order to take appropriate prevention actions, you should profile the users and conceive prevention products on shortened URLs which are addressed to a specific type of user or a specific type of user activity (i.e. social networking site, e-mails etc.). The Questionnaire is structured in two sections: general questions and specific questions.

A. General Questions

The general questions are aimed at defining the profile of the subject who is taking the survey. In order to achieve these two questions were devised; one connected to the amount of time the user spends on the Internet and the second on the area of interest while browsing.

The first question focuses on the time spent online since this can be an indicator as to the frequent use of multiple Internet services and the probability of using an URL shortening service.

The second question is aimed at identifying the frequent area of interest of the subjects who are taking part in the survey so that appropriate measures can be devised later in relation to cybercrime prevention material.

B. Specific Questions

The second part of the Questionnaire is composed of three groups of question that address three main issues: (i) the frequency of use of URL Shortening Services; (ii) user confidence as well as (iii) user awareness on the risks that one is exposed to when accessing a Shortened URL. Details of these questions are described as below.

The first group is intended to provide an understanding on how often and in relation to which Internet services (i.e. web browsing, social networking sites etc.) the subjects of the Survey make use of short URLs. The Internet services mentioned in the Questionnaire were added based on a previous paper [4] released in May 2011 referring to security implications of URL shortening services.

The second group approaches the user confidence in utilizing short URLs. One question attempts to identify the typology of URL shortening services a person is more at ease with using, either well known services or a specific shortening service. Another question is aimed at determining the subject's perception of the safety when using a short URL. Associated to this is one more question that inquires the subject as to how he or she perceives the measures taken by URL shortening services in order to protect users of Internet security risks (i.e. malware, spam etc.). The final question in relation to user confidence is a composite question made up of three different indicators with reference to a short URL, respectively stability, lifetime and popularity. The measurement of the indicators gives out an overall perception as to certain characteristics of short URLs which make them a better option of choice for Internet users.

The third group makes up the final part of the Questionnaire that addresses the subject's perception on the risks he or she is exposed to when utilizing short URLs. This group begins with a general assessment on the level of risk perceived by the subject of the Survey in relation to the use of short URLs. One question in this group touches upon the most frequent security risks associated with the use of short URLs (i.e. malware, phishing, spam) identified in previous papers as well as articles and it tries to determine the level of acknowledgement on the risks from the side of the survey subject. Another question goes one step further and puts into discussion the issue of specific software products installed on the subject's machine in order to avoid security risks when using short URLs. There are two questions that aim at creating a minimum level of awareness on the risk potential of short URLs through the examples of phishing and malware:

1) First question refers to an observation [10] included in the Global Phishing Survey of semester 2 of 2013 mentioning that approximately 51% of all of the malicious shortened URLs used for phishing were found at a single provider (i.e. tinyURL.com).
2) Second question refers to a situation from 2009 when the URL shortening service Cligs was hacked [11]. Yet, the hacking of the Cligs URL shortening service has puzzled security researchers. Instead of pointing to a spamming related site, the redirect was executed towards a harmless Register site. One of the theories explaining the strange redirect which was advanced by a senior technology consultant for SophoLabs was that the hacker rerouted users to the Orange County Register site by mistake. At the time of the hack, Cligs was ranked as number four most popular URL shortening service used on Twitter. Despite the inconvenience and possible loss of tens of thousands of URLs, security experts had said that the attack could have been much worse as the hackers could

have redirected millions of shortened URLs to a website hosting malware.

The final question in the third group addresses the important issue of protection measures that can be taken by users in order to avoid malicious security threats associated with short URLs. To this end, this question inquires about the suitability of a list of protection options which can be easily put into practice by users with basic IT skills, such as:

1) installing a Site Advisor software [12]
2) installing an Add-on in the web browser which allows the user to view the long URL instead of the shortened URL of websites;
3) previewing the web sites where short URLs redirect with specialized web services before accessing them.

Although the Questionnaire is conceived as one which should be accessible to Internet users with all levels of technical skills, for specific questions there is also an additional option mentioned in certain questions which is a free text option (i.e. "other, please specify...") which is aimed at more advanced Internet users who can give a more thorough description of their experience when using short URLs.

V. Evaluation and Analysis

A. Experiments

The Survey was applied on a number of 100 people in the age range 28 - 50. The nationality of the subjects was broadly distributed among the 28 European Union Member States.

The Questionnaire was distributed in electronic format over a period of 5 days.

As mentioned above, the Questionnaire was divided into a general questions section with a view of determining the subjects' preferences and Internet usage patterns as well as a specific questions section in order to address.

Following the distribution of the Questionnaire and the receipt of the filled in documents, the results were analyzed based on the initial three goals of the survey:

1) frequency of use;
2) user confidence;
3) user awareness;

When utilizing short URLs on the Internet.

Although all 100 people (so-called subjects) returned the filled in Questionnaire in electronic format, a number of 9 participants to the survey mentioned that they never use short URLs and therefore did not continue with filling in the Questionnaire. Hence, these 9 subjects only provided feedback on the first 3 questions of the survey.

Therefore a number of 91 subjects responded to all of the questions included in the survey, answers which will be analyzed in the following sections.

B. General Questions

Based on the answers to general questions by the participants to the Questionnaire, the following conclusions were made available on the subjects of the Survey.

The majority of the subjects 34% spend 1 - 2 hours daily on the Internet daily followed by 33% who spend 2 - 4 hours on the Internet. These figures provide an indication that the survey subjects are likely to provide an objective overview on the use of short URLs since they spend more time on the Web.

The second question addressed the issue of the frequent areas of interest on the Internet. The first 3 choices were made up of 34% of the respondents who provided feedback that they are interested in checking their e-mail accounts, 28% of the subjects who mentioned they are interested in news sites and 25% of the subjects who mentioned they have an interest in social networking sites (Fig. 1).

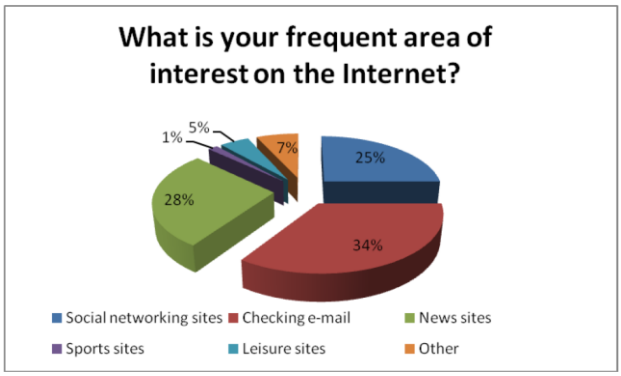


Fig. 1. Proportion of areas of interest on the internet.

Therefore any prevention material on the topic of short URLs should be addressed to these 3 categories of services.

C. Frequency of Use of Shortened URLs

When asked how often they use short URLs, out of the 100 survey participants, 55 responded that they rarely use these types of URLs, 21 responded that they use them every day, 15 provided feedback that they use them once every couple of days and 9 persons replied that they never use short URLs.

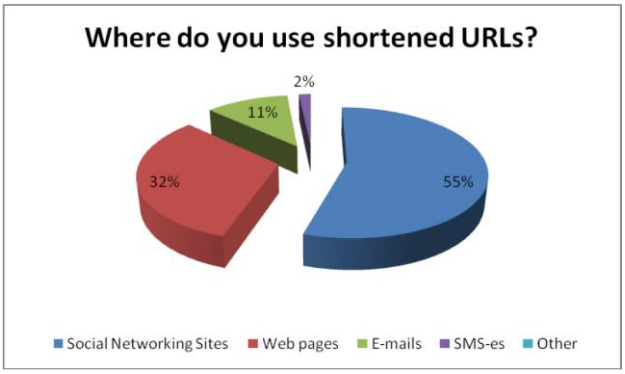


Fig. 2. Proportion of services where short URLs are used on the internet.

Out of the 91 persons who replied they use short URLs, the largest proportion 51% use them on Social Networking Sites followed closely by 32% of the subjects who use them while accessing various websites. This tendency is in line with the main aim of short URLs which was to counter restrictions imposed by Social Networking sites however it reveals an interesting development in the use of short URLs on other web pages and e-mails. Specifically this shows that the proportion of use of short URLs is propagating to other services on the Internet which means a higher coverage by short URLs and increased risks for users (Fig. 2).

In an attempt to identify the Social Networking Site where short URLs are more frequently utilized, 48% of the subjects use short URLs on Facebook (Fig. 3).

This proportion reflects on the one side the expansion of the social networking platform Facebook; however on the other side is a signal of the popularity of the short URLs which have begun to be adopted equally by other platforms.

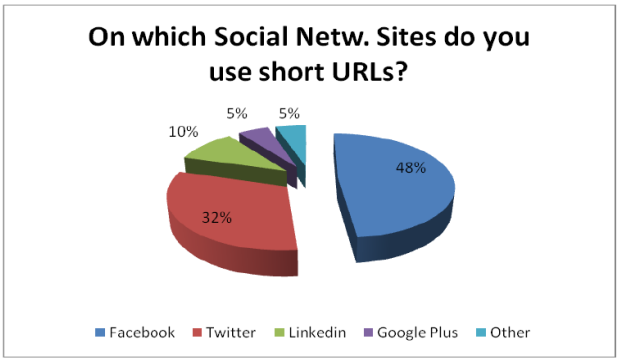


Fig. 3. Proportion of social networking sites where short URLs are used.

D. User Confidence in Accessing Short URLs

In terms of user confidence when it comes to shortening services providers, the participants were quite straight forward.

When asked which short of URLs they are more confident in using, 70% of the Survey participants answered that they feel more confident in using URLs from well-known shortening services (i.e. goo.gl, bit.ly, t.co, ow.ly, tinyurl.com) and the rest of the subjects mentioned that it doesn't matter which URL shortening service the link refers to.

This could be an indication for the URL shortening services with the highest number of accessed links to step up their measures in providing safe URLs for their users.

An important observation as to user perception of safety when utilizing short URLs can be seen in the replies to question related to the ranking of using short URLs. None of the subjects ranked the safety a very good. Out of the 91 subjects who use short URLs, the majority of the respondents - 42 - pointed out that the safety can be ranked as moderate followed by 33 subjects who ranked it as poor (Fig. 4). This shows a certain user awareness as to the risks which can occur when utilizing short URLs.

The following question addresses the people perception on the measures taken by URL shortening services to deliver risk free short URLs. Approximately 57% of the survey participants rated the measures as moderate and approximately 30% considered the measures as poor.

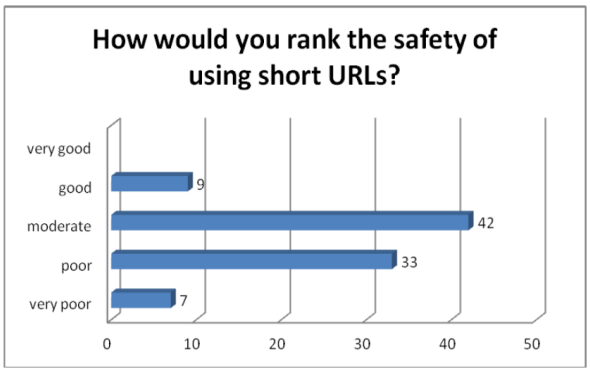


Fig. 4. Ranking of safety in relation to utilizing short URLs by users.

As mentioned above, one of the question inquires user opinions on three characteristics of short URLs specifically stability, lifetime and popularity, which are indirectly related to user confidence. Although when asked how they would rate the stability and lifetime of short URLs, the majority of participants to the Survey rated them as moderate, in terms of popularity of short URLs most users rated them as good - 46% and 18% rated them as very good (Fig. 5).

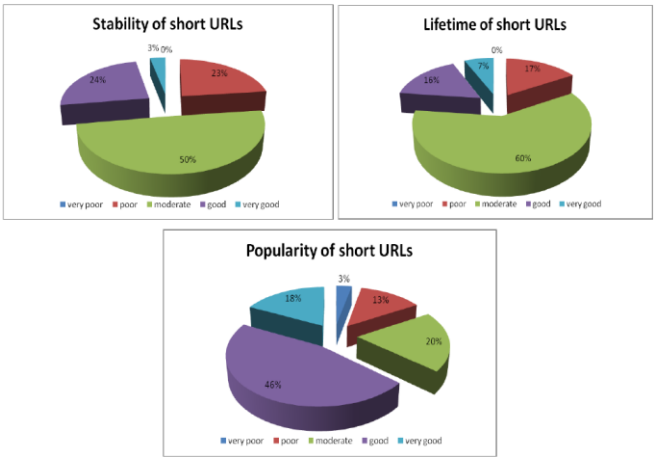


Fig. 5. Rating of stability, lifetime and popularity of short URLs.

From the assessments of the three characteristics and corresponding charts, we can draw the conclusion that users are not currently very concerned about the stability and lifetime of short URLs; however they do agree that these types of URLs are popular. This aspect would leave room for significant improvement in future awareness papers on short URLs to focus on the issue of stability (i.e. broken links etc.) as well as lifetime (i.e. availability of the short URL).

E. User Awareness When Using Short URLs

As mentioned in the previous chapter of the paper, the final part of the Questionnaire addresses the issue of user awareness on the risks that one is exposed to when accessing a Shortened URL.

Based on the replies of the subjects, out of the 91 users of short URLs, 45 of the respondents (approximately 49%) considered the risk moderate, however an important number of participants — 30 (approximately 33%) found the risks as high and 8% considered the risk as very high (Fig. 6).

Going into detail on the risks associated with short URLs, the subjects of the Survey were asked to identify the potential threats linked to the use of short URLs.

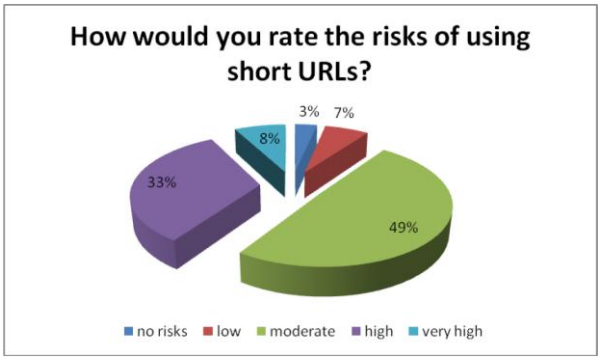


Fig. 6. Rating of risks perceived in relation to the use of short URLs.

The majority of the respondents pointed out that phishing

attacks would be more frequent with 38% of the respondents indicating them as the prevalent threat, followed by spam in proportion of 34% and malware attacks with 27% (Fig. 7).

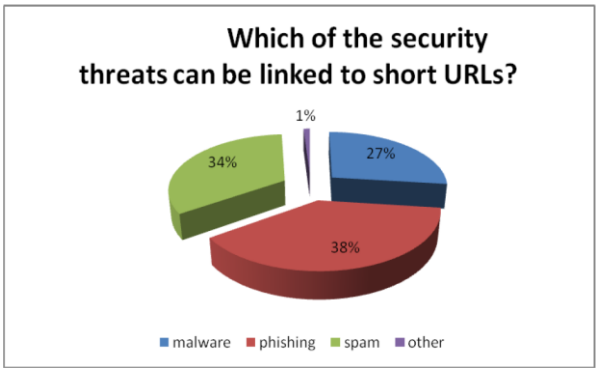


Fig. 7. Proportion of possible threats linked to short URLs.

Although the survey participants have identified in the previous question several key threats to IT security when accessing short URLs, the majority of subjects — 74% still believe that their Antivirus software is sufficient to counter any risks associated with the use of short URLs. The remaining 26% of the respondents provided solutions such as the use of virtual machines, Norton Safe Web software [13], McAfee Site Advisor [12], Bitdefender TrafficLight [14], Quttera URL Scanner [15]. The other questions in this group are inter-related in the sense of presenting situations to the participants to the survey, which are representative for abusing URL shortening services.

The situations refer to:

1) An observation included in the Global Phishing Survey of semester 2 of 2013 mentioning that approximately 51% of all of the malicious shortened URLs used for phishing were found at a single provider (i.e. tinyURL.com);
2) The account that in 2009 a URL shortening service (i.e. Cligs) was hacked which lead to 2 billion shortened URLs re-directed to a single web page.

The conclusion is that an overwhelming majority of users, 90% in the first situation and 84% in the second situation, are not aware of concrete cases involving abuses of URL shortening services.

Although knowledge of these situations is not a pre-requisite for all Internet users, such concrete examples of short URL abuse should be included in any material aimed at the general public reflecting the risks of short URLs.

The final question of the survey attempts to establish the preferred modalities of users to protect themselves from the risks associated to short URLs.

The majority of the participants to the survey — 46% mentioned they would be more comfortable in installing a Site Advisor software, probably because this is the most practical solution as aside from installation it does not require additional measure to be taken by the user.

The following option according to the respondents to the survey — 31% would be installing an Add-on in their browser to allow the user to visualize the complete URL when "surfing" the Internet, yet this solution is not very widely accepted since it can be limited to a specific Internet browser. The third option chosen by the subjects — 18% was previewing the web sites where shortened URLs redirect with specialized web services before accessing them (Fig. 8).

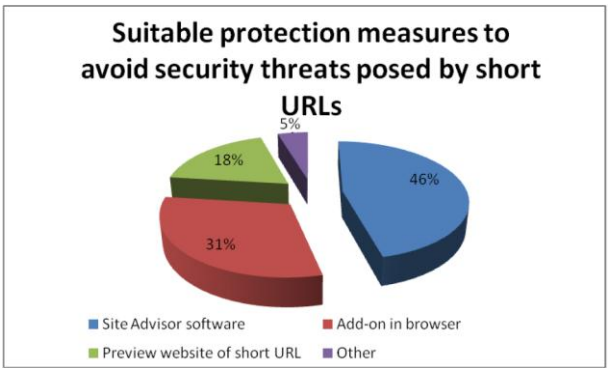


Fig. 8. Proportion of protection measures considered measures considered suitable by users in order to avoid security threats.

Given the answers provided, we can draw the conclusion that users prefer to have a solution which integrates all security protection measures from short URLs in one piece of software which is compatible with a variety of Internet browsers.

F. Further Analysis

The Questionnaire on the use of URL shortening services provides a baseline assessment as to how Internet users currently interact with shortened URLs and what is their perception on the frequency of use, user confidence and user awareness when utilizing short URLs.

In terms of frequency of utilizing short URLs, these types of URLs are apparently rarely used while browsing the Internet. However there is an important development noticed in the areas where the short URLs are used, specifically that although the main aim of short URLs was to counter restrictions imposed by Social Networking sites, the use of short URLs is propagating to other services on the Internet (i.e. normal web-pages and e-mails) which means a higher coverage by short URLs and increased risks for users.

In terms of user confidence, the Questionnaire proves that there is a general awareness by the users that accessing short URLs is not perceived as a completely safe action when browsing the Internet. Users apparently feel more confident in using URLs from well-known shortening services (i.e. goo.gl, bit.ly, t.co, ow.ly, tinyurl.com). This could be an indication for the URL shortening services with the highest number of accessed links to step up their measures in providing safe URLs for their users.

In addition, users are not currently very concerned about the stability and lifetime of short URLs, however they do agree that these types of URLs are popular. This aspect would leave room for significant improvement in future awareness papers on short URLs to focus on the issue of stability (i.e. broken links etc.) as well as lifetime (i.e. availability of the short URL).

In terms of user awareness, the survey reveals that the majority of users still perceive the risks posed by short URLs as moderate followed closely by another category of users who perceive the risks as high. Although the Survey participants have identified several key threats to IT security (i.e. phishing, spam, malware) when accessing short URLs,

the majority of subjects - 74% still believe that their Antivirus software is sufficient to counter any risks associated with the use of short URLs. There is however a small proportion of users who are taking a proactive approach in avoiding risks of short URLs by installing different software applications such as Norton Safe Web software, McAfee Site Advisor, Bitdefender TrafficLight, Quttera URL Scanner or an Antivirus software with Total Security (including web surfing, site advisor).

As observed from analyzing the answers to the Questionnaire, an overwhelming majority of users are not aware of concrete cases involving abuses of URL shortening services. Although knowledge of these situations is not a pre-requisite for all Internet users, such concrete examples of short URL abuse should include in any material aimed at the general public reflecting the risks of short URLs. Another observation based on the user awareness section of the Questionnaire is that when it comes to the preferred modalities of users to protect themselves from the risks associated to short URLs, most of them are inclined to adopt a solution which integrates all security protection measures from short URLs in one piece of software which is compatible with a variety of Internet browsers (e.g. a Site Advisor software).

In addition, based on the General questions section of the Survey we can draw the conclusion that opposite to the current tendency that awareness material on the risks of using short URLs is usually published on IT security sites, such prevention material would yield better results if published on the platforms of e-mail clients, news services and social networking sites as these are the common areas of interest of users on the Internet. Based on the feedback received from the participants to the Survey, an observation can be made that the Questionnaire can prove to be a valuable tool for compiling prevention material aimed at users of short URLs.

VI. Conclusion and Future Work

As a final conclusion it can be pointed out that there is a general awareness that the use of short URLs is associated with security risks while browsing the Internet. Furthermore there is a remote category of users who are taking additional measures to protect themselves against risks of short URLs. However the lack of user awareness on concrete threats (i.e. actual cases of short URL abuse) as well as the lack of a strategy in disseminating prevention material on platforms which are frequently used (i.e. e-mail clients, news services, social networking sites) can cause substantial problems in the future especially with the expansion of short URLs to other Internet services and platforms.

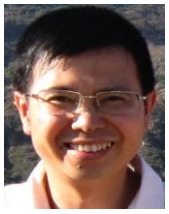
More surveys are being carried out. We are moreover analyzing and extracting knowledge related to the users' perspective on using short URLs and handling these knowledge with our knowledge map [16], [17].

Acknowledgment

This research is conducted by one of the MSc FCCI students, any comment or feedback please contact cci@ucd.ie or an.lekhac@ucd.ie.

References

[1] URL shortening. [Online]. Available: http://en.wikipedia.org/wiki/URL_shortening
[2] A. Neumann, "Analyzing security implications of URL shortening services," Diploma Thesis, RWTH Aachen University, 2011.
[3] F. Maggi, A. Frossi, S. Zanero, G. Stringhini, B. Stone-Gross, C. Kruegel, and G. Vigna, "Two years of short URLs internet measurement: Security threats and countermeasures," presented at the Intl. World Wide Web Conference (WWW), Rio de Janeiro, 2013.
[4] A. Neumann, J. Barnickel, and U. Meyer, "Security and privacy implications of URL shortening services," presented at the Web 2.0 Security and Privacy 2011 Conference, Oakland, USA, May 2011.
[5] D. Antoniades, E. Athanasopoulos, I. Polakis, S. Ioannidis, T. Karagiannis, G. Kontaxis, and E. P. Markatos, "Web: The web of short URLs," presented at the 2011 Intl. World Wide Web Conference (WWW), Hyderabad, India, March 2011.
[6] AI. Iversion. (March 2011). Spamhaus and URL shortening services. *Spam Ressource*. [Online]. Available: http://www.spamresource.com/2011/03/spamhaus-url-shortening-services.html
[7] MX Lab. (January 2011). Increase in usage of URL shorteners in spam campaigns. [Online]. Available: http://blog.mxlab.eu/2011/01/04
[8] D. Lauretti, "Facebook is blocking links from Google's URL shortening service," *Examiner*, March 2013.
[9] MX Lab. (July 2009). Shortened URLs: The real dangers behind and how to avoid troubles. [Online]. Available: http://blog.mxlab.eu/2009/07/17/
[10] G. Aaron, R. Rasmussen, and A. Routt, "Global phishing survey: Trends and domain name use in 2H2013," *APWG Industry Advisor*, MA, USA, April 2014.
[11] S. Hoffman, "Cligs URL shortening service hacked, users redirected," *CRN Technology News for Solution Providers and the IT Channel*, p. 1, June 2009.
[12] M. Rajab, L. Ballard, N. Lutz, P. Mavrommatis, and N. Provos, "CAMP: Content-agnostic malware protection," presented at the 20th Annual Network & Distributed System Security Symposium, CA, USA, February 24, 2013.
[13] M. Merritt, *Family Online Safety Guide*, 4th ed. Norton Symantec Press, December 2012.
[14] C. A. Consoi, "Dealing with image spam," *Virus Bulletin*, pp. 1-3, December 2006.
[15] R. Fry, "Malware defense and automation: Fully integrated defense operation," presented at the RSA Conference, February 24-27, 2014.
[16] N-A. Le-Khac, L. M. Aouad, and M. T. Kechadi, "Knowledge map: Toward a new approach supporting the knowledge management in distributed data mining," presented at the 3rd International Conference on Autonomic and Autonomous Systems, Athens, Greece, 2007.
[17] N. A. Le-Khac, M. T. Kechadi, and J. Carthy, "ADMIRE framework: Distributed data mining on data grid platforms," presented at the International Conference on Software and Data Technologies, Setubal, Portugal, September 11-14, 2006.



Nhien-An Le-Khac is a lecturer at the School of Computer Science & Informatics (CSI), University College Dublin, Ireland. He obtained his Ph.D. degree in computer science in 2005 from the Institute National Polytechnique Grenoble (INPG), France. His research interest spans the area of data mining/distributed data mining for security, fraud and criminal detection, cloud security and privacy, grid and high performance computing.

M. Tahar Kechadi received his PhD degree in computer science from University of Lille I, France. He was appointed as a lecturer at the Computer Science Department of Lille University. He joined UCD in 1999 as a permanent staff member of the School of Computer Science & Informatics (CSI). He is currently a professor of computer science at CSI, UCD. His research interests span the areas of distributed data mining healthcare data analytics, grid and cloud computing, and digital forensics and cyber-crime investigations. Prof. Kechadi has published over 265 research articles in refereed journals and conferences. He serves on the scientific committees for a number of international conferences. He is the editor-in-chief of Journal of Computer Science of Science Publications. He is also an associate editor of the Journal of Future Generation of Computer Systems.