Cyber Attacks, Countermeasures, and Protection Schemes– A State of the Art Survey

Antesar M. Shabut
Anglia Ruskin University
Chelmsford, UK
antesar.shabut@anglia.ac.uk

K T Lwin
Anglia Ruskin University
Chelmsford, UK
khin.lwin@anglia.ac.uk

M A Hossain
Anglia Ruskin University
Chelmsford, UK
alamgir.hossain@anglia.ac.uk

***Abstract*— Thousands of cyber-attacks (fraudulent online activities to acquire users' sensitive information via email, during online transactions, live video streaming, online gaming and browsing) are launched every day against Internet users across the world. To prevent these attacks, researchers have responded with a number of protection systems. Currently, the methods which cyber-attackers use to conduct attacks is associated with exploiting humans. Such attacks are recorded more frequently than before, and they are more challenging to control. Traditional security countermeasures are unable to prevent breaches targeting the human element. This paper describes the state of the art of cyber security attacks, countermeasures, and protection tools related to everyday online activities. It provides a useful cyber-attack taxonomy and classification which helps to involve in a protection process to identify attacks and measures for cyber security. Existing protection schemes that target the cyber threats and risks are evaluated against three of our criteria for an effective measure: resilience to cyber-attacks' countermeasures; real-time support and needs-based action; and training and educational materials to increase users' awareness of cybercrimes. Potential features of smart solutions to cybercrime are also identified.**

Keywords—cyber security; cyber attacks; attack taxonomy; existing protection tools

I. INTRODUCTION

Cyber-attacks have become more frequent and costly to individual users, businesses, economies and other critical infrastructure components. Symantec discovered more than 430 million new unique pieces of malware in 2015[1], 91% of attacks started by using phishing techniques, while numerous high-profile breaches originated from a single phishing attack [2]. New ransomware evolves its approaches of propagation, encryption, the victims it seeks, and the means of distribution, including Internet chat, peer-to-peer networks, newsgroup postings, and email spam on a daily basis. [3]. Traditional security tools such as anti-virus measures are unable to prevent all cyber-attacks, and particularly unknown ones. Developing the users' ability to detect, prevent and defend against cyber-attacks is important factor because humans are considered the weakest link in the current interconnected world and most security breaches are due to human performance [4]. A recent research reported that 93% of breaches were due to human error [5] while 95% of data loss was due to cultural factors [6]. It is evident that critical security incidents occur due to users' unintentional mistakes, errors, culture and knowledge which are not considered properly by current security schemes. The enhancement of existing cyber security schemes to create better user awareness, advice, and response to cybercrime will be required. Increasing users' implicit and explicit knowledge of current and upcoming attacks is also an important requirement.

Several protection tools are proposed to improve safety behaviour and promote the confidence of users to become involved in online activities. Cyber security protection systems are mainly based on the use of three techniques: blacklists, heuristics or a hybrid. Blacklist based techniques cannot cope with zero-day cyber-attacks and rapid recycling of blocked attacking pages. Web browsers' filters [7][8] are an example of blacklists which block phishing web pages by comparing URLs against known phishing sites stored locally on the user's machine or in a remote database. Meanwhile, heuristics based techniques rely on decision rules which are difficult to apply in a way which seems consistent to human perception. CANTINA [9] is an example of a heuristics based technique which blocks phishing web pages based on features extracted from them. Hybrid based techniques use both blacklists and heuristics to cope with cyber-attacks. GoldPhish [10] is an example of a hybrid phishing detection technique which utilises an optical character recognition (OCR) technique to detect phishing webpages. Such techniques are used to extract text from images found on web pages, such as the company logo, and then to leverage the Google PageRank algorithm to help render a decision on the validity of these webpages. However, such techniques can suffer from the drawbacks of both blacklists and heuristics based techniques.

Potential protection by any security system requires standards when disseminating cyber vulnerability information to allow analysis of multiple cyber vulnerabilities of users [11]. It is important to provide users with a holistic picture of cyber space to include information about types of attackers and possible attacks, motives and drivers, and the targets and consequences of cybercrimes. There are still open and challenging problems for existing protection tools to leverage best practices, define terminology, classify and identify dimensions used by cyber space standards to populate attack forms, as well as training and education metadata. Cyber-attack taxonomy and classification can help users involved in a protection process not only to identify attacks, but also to identify measures to prevent, mitigate and remediate cyber vulnerabilities. Planning and exchange of cyber information via cyber

978-1-5090-3298-3/16/$31.00 ©2016 IEEE

security technical forums, social media or other kinds of sharing methods is noteworthy to consider for existing protection tools.

Cyber-attacks are expected to increase in number and sophistication in the future. Therefore, existing protection tools are not able to intercept attacks such as drive-by download because these attacks become more sophisticated and well-organised [12]. Smart detection techniques that solve existing cyber problems are needed [13]. A combination of different techniques which use human factors as a basis, along with the heuristics-based approach can, as long as standardized historical data is available, deliver an effective intelligence based protection scheme to help users make a good real time decision. Our contributions in this paper include: (a) providing the state of the art in the cyber security field of study and its importance in everyday online activities; and (b) presenting a useful cyber-attack taxonomy and classification to help users involved in a protection process to identify attacks and measures to prevent, mitigate and remediate cyber vulnerabilities. The taxonomy includes information about type of attackers and possible attacks, motives and drivers, targets and consequences of cybercrimes. (c) Unlike previous research, existing protection systems which target cyber threats and risks are evaluated against three of our criteria for an effective anti-cyber-crime system; resilience to cyber attacks' countermeasures, real-time support and needs-based action, and training and education materials to increase users' awareness of cybercrimes. This evaluation can help researchers in the cyber security field of study to propose useful and effective protection schemes for current and upcoming attacks.

The remaining parts of this paper are organised as follows. Section II gives an overview of the various types of cyber-attacks. Section III provides a comprehensive review of existing protection tools. Section IV presents a recommendation for cyber security researchers to build a smart protection tool. Conclusions of the paper are provided in Section V.

II. Various Types of Cyber Attacks

Cyber-attack is one of the most rapidly growing threats to the interconnected world of information technology [14]. These are computer-based attacks which exploit human vulnerabilities rather than software vulnerabilities. Phishing email or phishing webpage is a type of cyber-attack in which victims are sent emails or fake webpages with links which deceive them into providing sensitive information such as account numbers, passwords, or other personal information to an attacker. Collecting information about victims can make phishing more convincing and allow it to falsely relate to a reputable business where victims might have an account. Victims are directed to a spoofed web site controlled by an attacker where they enter sensitive information such as credit card numbers. Drive-by download is a malicious piece of software which works by exploiting vulnerabilities in web browsers, plug-ins or other components that work within browsers to distribute malware without the victim's knowledge. The downloaded malware may use the victim's actions or automatically conduct malicious actions such as stealing users' personal identification or password, joining a botnet to send spams, hosting a phishing site or launching distributed denial of service attacks [15]. Social engineering is also a kind of attack which exploits human behaviour to act on malicious intentions: especially on social networking sites. In addition, there are currently more cyber-attacks associated with exploiting humans than previously recorded, and these are more challenging to classify and control. It is a significant global challenge for information security to protect confidentiality, integrity and availability of information. Cyber-attack taxonomy and classification can help users involved in a protection process not only to identify attacks, but also to identify measures to prevent, mitigate and remediate cyber vulnerabilities. Several researchers have contributed to the knowledge of cyber-attack taxonomy and classification in order to help users become aware of cyber threats/risks associated with online activities [11], [16]–[18]. In this section, we provide a holistic view of some known cyber-attacks in computer security. It includes information about types of attackers and possible attacks, motives and drivers, targets and consequences of cybercrimes. The holistic approach taken is provided in Fig. 1.

III. Existing protection Tools

There has been a number of tools proposed as a response to the increasing number of attacks launched every day affecting Internet users across the world. In this section, an overview of various protection tools is given. A taxonomy and classification of existing techniques are also provided. Fig. 2 shows the classification of existing protection tools based on the technique used to cope with evolving cyber threats/risks. In this paper, we only focus on technical and non-technical tools.

A. Non-Technical Tools

Legislative Tools: The United States was the first nation to use laws against cyber activities, and many cyber attackers have been arrested and sued. The Cybersecurity Act of 2015 in the United States signed a number of measures into law on December 18, 2015 [19]. The Act aims to defend against cyberattacks by creating a framework for the voluntary sharing of cyber threat information between private entities and the federal government, as well as within agencies of the federal government. Several countries have followed the United States, and Australian and UK governments have strengthened their legal arsenal against fraud by prohibiting the development of cyber activities and setting penalties, including jail terms. The UK Cyber Security Strategy [20] aims to tackle cyber-crime and make the UK the safest place in the world in terms of resilience to cyber-attacks. Further, it is used to set out which departments are responsible for specific actions. For example, the Home Office leads on cyber-crime and the Foreign and Commonwealth Office (FCO) on international cyber security. Budapest is the name of the Convention on Cybercrime which was drafted by the

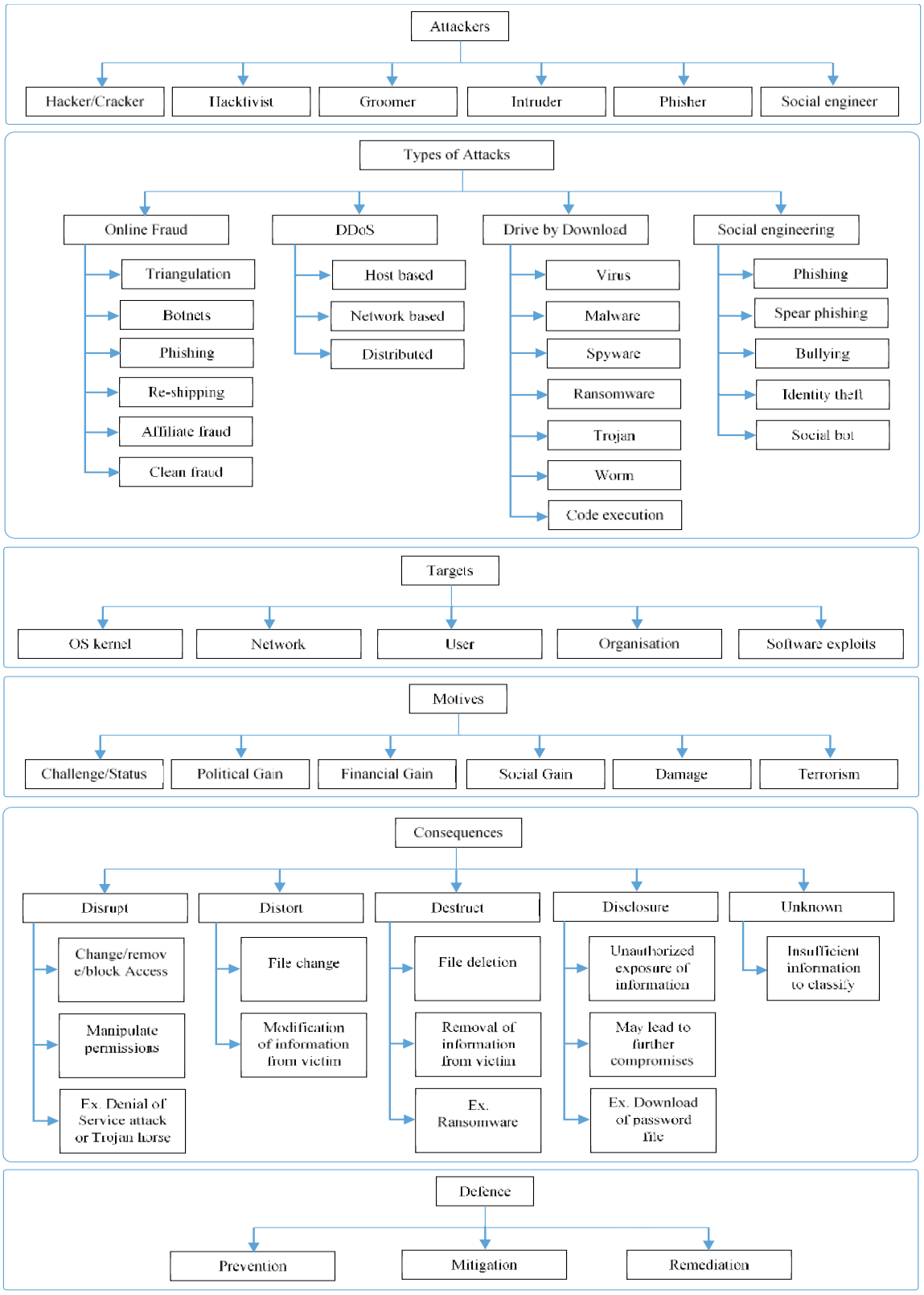

Fig. 1. Cyber Attacks Holistic View

Council of Europe (COE) in Strasbourg, France [21]. The Convention seeks to internationally harmonize national laws on cybercrime and improve national capabilities for investigating these crimes, as well as to increase capacity for cooperation on investigations. However, legal solutions are insufficient in catching cyber attackers, since it is very difficult to trace such criminals due to their quick disappearance in the cyber world, and the use of developing countries where laws to defend against cyber-attacks are weak or where there is no relevant legislation.

- *Training and Education Tools*: Protecting the confidentiality, integrity and availability of information is a significant global challenge for information security. Organisations and individual users suffer from lack of knowledge about cyber-attacks. A new cyber security knowledge platform from ISACA, the Cybersecurity Nexus (CSX) programme [22], is responsible for providing security professionals with the knowledge, guidance and tools they need to help them be effective at their job. Monitoring of legislation for cybersecurity to keep professionals up to date with developments in cyberspace is also provided by this programme. In addition, it provides training and certification for those professionals in cyber security to lead their organisations towards a safe environment. Campaigns such as "Be Cyber Streetwise" [22] and "make the UK a safer place to conduct business online" [23], which have recently been issued in the UK by Government, with the aim of significantly improving safety behaviour in online activities and promoting confidence in individuals and organisation. Their purpose is to prevent cyber-attacks by utilising training, planning and exchange of information via cyber security technical forums or social media. Although training and education is the most important factor in defending against cyber-attacks, issues like engagement, quality of materials and time and the method for delivering materials are still open and challenging tasks. Techniques such as serious games for cyber security that utilise gamification of training and education for cyber security will be beneficial [24]. Serious games based training and education for cyber security will be discussed in Section 3.2 on technical tools.

B. *Technical Tools*

In this subsection, we will provide an overview of technical protection tools used to cope with cyber-attacks, with contexts ranging from industry to academia. The techniques, strengths, and weaknesses involved in these tools are also explored. Table I gives a comparative study of cyber-attack detection technical tools.

The conventional approach used by most Internet users to protect themselves is to use anti-virus software. However, with increasing numbers of cyber-attacks, sophisticated and well-organised strategies in designing such attacks, besides time between an incident being detected and anti-virus vendors providing protection against the new threats often spanning hundreds of days, it is difficult for conventional protection tools, such as anti-virus software, to keep pace.

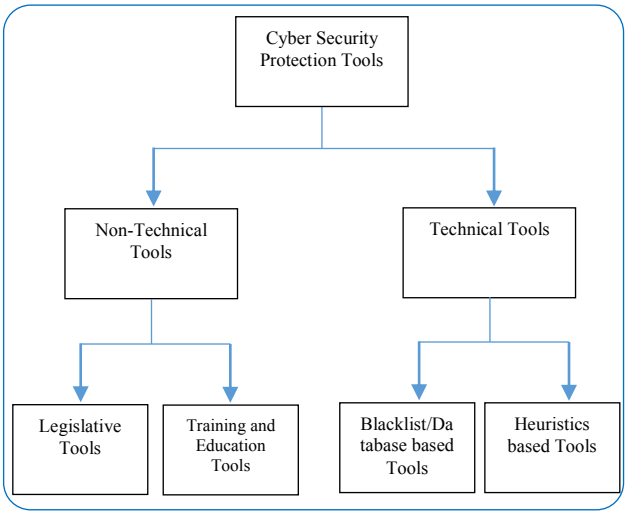

Fig. 2. Protection Systems Techniques

Big brand Internet security products such as MacAfee LiveSafe [25] attract a large number of users because of their features. These tools warn users of suspicious web pages and, as part of an anti-theft regime, can take photographs and wipe data remotely. There is also use of encrypted password management via SafeKey and Personal Locker. Having these capabilities is useful for users who have knowledge about online threats, costs, and countermeasures and in turn can respond to security warnings. A high number of users however ignore security warnings (e.g. when they use PayPal for an online purchase or even posting or sharing a link on online social networks) because they have no knowledge or training regarding potential threats, and the warning message may be difficult for them to understand. So, it is important to educate users, to improve awareness of threats, risks, and what security warnings are about. Social-psychological research on cyber security has identified that ineffective cognitive processing is a key reason for users to be victimized [26]. Security tools need to focus on training users to better understand their vulnerabilities and in turn detect cyber activities.

Web browser filters such as PhishTank SiteChecker [7] protect Internet users against phishing and malware based on the blacklist technique by comparing the currently-requested URL against a database of known fake web pages. The filters notify user of results regarding whether the URL is legitimate or fraudulent by sending a request to a remote database. It is common that blacklists depend on human intervention to verify suspicious URLs before adding them to the blacklist, and in turn this may give cyber attackers a chance to reach their goals. Web browser filters protection tools fail to satisfy our main criteria of being resilient to cyber-attack because of the response of phishers in quickly recycling phishing pages onto a new domain. The short lifetime of fraudulent web pages makes it difficult for

blacklist filters to detect them, with several days between launch and takedown. Further, maintaining a huge blacklist of fraudulent URLs and frequently updating it is a challenging task.

The Google Safe Browsing system [8] for anti-phishing is based on certain URL and client-side checks. When Safe Browsing is enabled, the most recent Safe Browsing list (containing unsafe sites) is periodically downloaded and stored locally on the user's system. However, Google Safe browsing has been largely criticised for its privacy-unfriendly by design. Google stores another cookie on the user's computer, which can be used to identify the IP addresses which the user visits: i.e. it can be used to track him or her. According to the Google Chrome Privacy Whitepaper [27], Google logs the transferred data in its raw form for up to two weeks. It collects standard log information in connection with Safe Browsing requests, including an IP address and one or more cookies. These logs are also tied to other Safe Browsing requests made from the same device. Existing safe browsing tools and especially web browsers are therefore exposed to several privacy threats [28].

Another design weakness is that for example Google Safe Browsing does not block any phishing URL when the synchronization step is skipped [29]. Considering that some users may not frequently synchronize their devices, this may result in an outdated blacklist. Thus, in the meantime, any phishing site that has been created, even if it has been reported to the Safe Browsing list, represents a risk to users who utilise such a tool to fight against cyber threats [29]. Also, the amount of time taken by Google's API is large (approximately 80ms for Google, excluding the time taken by an end user to download the Google blacklists locally), and besides, there is no limit on the response time by the lookup server [30].

The Phishing Initiative protection tool [31] is a European project that protects a company or administration against cyber-crime with the aim of helping them fight fraudulent web pages stealing identities. The Phishing Initiative uses the same technique as Google of blacklisting suspicious web pages based on a remote database of known fraudulent web pages, and in turn inherits its weaknesses. It allows an organisation's users to submit suspicious phishing URLs and then send them over to CERT-LEXSI's expert teams for analysis. The final step includes, where necessary, undertaking relevant countermeasures to add confirmed fraudulent web pages to blacklists.

Spoofguard [32], the CANTINA toolbar with Internet Explorer [9] and Mozilla Thunderbird [33] are protection tools based on heuristic techniques that block fraudulent web pages based on features extracted from them. The heuristics used in these tools are machine learning models which are presented as black boxes, and with no clear explanation of how a web page is classified as a phish. The main drawback of such tools is their use of decision rules that cannot be consistent with human perception. Therefore, they incorrectly identify many legitimate web pages as fraudulent, and have them blocked and shown as phishing pages. High false positives can reduce the confidence of users in protection tools and cause the disregarding of security warnings. The use of simple heuristics without study of human behaviour is insufficient to fulfil the online-based-needs of users with regard to trust, identity, privacy and security.

Design weaknesses also exist in mail clients' spam filtering tools, such as Mozilla Thunderbird, which receives mail before filtering. Therefore, spamming activities still exist, and the waste of Internet bandwidth and the storage space of mail servers due to spam messages also still exist. Spamming bots can be detected by such tools and addressed on the sender side as early as possible. Thus, the number of spam messages can be significantly reduced [34].

Another heuristics-based approach proposed in [35] depends on experimentally contrasting rules based classification algorithms using fuzzy data mining techniques to assess and identify phishing websites after collecting dissimilar features from a range of websites. Fuzzy data mining techniques can offer a more natural way of dealing with quality factors rather than exact values. A number of features are assessed to take one of three uncertain values: "Genuine'', ''Doubtful'' and "Fraud". The fuzzy data mining phishing website model shows a significant and important association of the "URL" and "Domain Identity" phishing website criteria. However, no justification is given of the way in which features have been assessed. The authors use a large set of features to predict whether websites are legitimate or not, and their methods show promising results in accuracy. However, design ambiguity in this method exists, in which the way that human factors-based features are extracted from the websites is not revealed. Besides this, the rules used were established based on human experience rather than intelligent data mining techniques. Lastly, the authors classify websites as very legitimate, legitimate, suspicious, phishy or very-phishy, but do not clarify the fine line that separates one class from another.

A Neuro-Fuzzy model based on the use of advanced techniques is developed in [36] to identify and extract phishing features based on five inputs: namely, Legitimate site rules, User-behaviour profile, PhishTank, User-specific sites and Pop-Ups from Emails. From these inputs, 288 features are extracted, which are used as training and testing input data for the Neuro-Fuzzy system to generate heuristics, and to discriminate between phishing, suspicious and legitimate sites in real-time. The method aims to make users more secure and build their confidence in online transactions. The authors provide a comparative study to demonstrate the merits of the proposed approach in terms of maximizing the accuracy of performance and minimizing false positives and operation time. Further, the authors claim that the use of a large number of features has the benefit of differentiating between phishing, suspicious and legitimate sites more accurately. Two main challenges associated with the use of the Neuro-Fuzzy Inference System are indicated by the authors themselves, in that it is complex and only gives a single output obtained using weighted average defuzzification, and besides this all output membership functions must be of the same type, either being linear or

TABLE I
COMPARATIVE STUDY OF CYBER-ATTACKS DETECTION TECHNICAL TOOLS

Cyber-attacks detection technical tools	Technique	Real time	Zero-day attack detection	Alert of phishing	Awareness & education	Other features
MacAfee LiveSafe [25]	Whitelists, blacklists & heuristic-based	Yes	Yes	Yes	No	Takes photos and wipes data remotely. Use of encrypted password management. Detection in real time. Firewall is not fully protected. Awareness and warning are not simple to understand.
Google Safe Browsing [8]	Blacklists-based	No	No	Yes	No	Human intervention is required. Maintaining and updating a huge blacklist. Synchronization is required. High operation time. Detection rate is low. Few or no false positive.
PhishTank SiteChecker [7]	Blacklists-based	Yes	No	Yes	No	Human intervention is required. Maintaining and updating a huge blacklist. High operation time. Detection rate is low. Few or no false positive.
Phishing initiatives protection tool [31]	Blacklists-based	Yes	No	Yes	No	Use of a third party expert for phishing analysis. Human intervention is required. High operation time. Few or no false positive.
Spoofguard [32]	Heuristic-based	Yes	Yes	Yes	No	Decision rules are not consistent to human perception. Detection rate is high. High false positive rate.
CANTINA toolbar [9]	Heuristic-Based	Yes	Yes	Yes	No	Decision rules are not consistent to human perception. Detection rate is high. High false positive rate.
Mozilla Thunderbird [33]	Heuristic-based	Yes	Yes	Yes	No	Decision rules are not consistent to human perception. Lack of real time accuracy. Receive mail before filtering. High false positive rate.
Intelligent Phishing Website Detection [35]	Heuristic-based (Fuzzy data mining)	No	Yes	No	No	Insufficient phishing features. Identify the importance of URL & Domain Identity. Real-life effectiveness is unclear. Detection rate is high. High false positive rate.
Intelligent phishing detection and protection scheme [36]	Heuristic-based (Neuro-Fuzzy model)	Yes	Yes	No	No	Sufficient phishing features. Real-life effectiveness is unclear. Detection rate is high. Low false positive rate. Gives better results than [9], [30].
Anti-phishing Phil [32], CyberCIEGE [38] and BigAmbition [39]	Serious game-based	No	No	No	Yes	Increases user awareness of cyber space. On-line based. Free and available for non-commercial use.
Phishing Education Landing Page [40]	Heuristic-based	Yes	Yes	Yes	Yes	Use of a landing page to alert users. Use of a third party to redirect suspicious URL to the landing page.

constant. However, for the two methods discussed above [35][36], it is unclear how effective such approaches are in mitigating phishing attacks in real life. Training and education is also missing.

Anti-phishing Phil [37], CyberCIEGE [38] and BigAmbition [39] are protection tools that have been proposed in industry and academia to educate users to improve their awareness of cyber-crime, and in turn change their behaviours and reduce risk. Further, these systems aim to increase awareness of cyber space, including attacks and defences in a virtual environment, with the objective of reproducing real life experience. In this context, these tools cannot satisfy the online-based-needs criterion in which it is significant for users to experience real life by using an innovative tool to monitor users' behaviours, actions and identify users' real-time needs and feed these into the gamified education system. When users are able to sense a real threat, they will have strong motivation to educate themselves and effectively engage in the gamified education system.

The Phishing Education Landing Page Program (PELPP) [40] is a protection tool developed by the Anti-Phishing Working Group (APWG) to train users on how to prevent themselves from being victimised by phishing attacks. The protection tool works when users click on a phishing link, with the users in turn redirected to a landing page which provides training material on how they can avoid being victimised in future, as a way of alerting users to the threat. This protection tool can satisfy the criteria of being resilient to cyber-attack countermeasures and of real-time support to provide education and training at the most teachable moment, when users encounter a phishing attack. However, this tool cannot satisfy the needs-based action criteria of users to automatically customise their training, security needs, and preferences by employing intelligent capabilities. This tool also suffers from the involvement of a third party (ex. ISP), which is required by PELPP to redirect any suspicious URL to the anti-phishing training webpage.

IV. Smart Protection Tool Features

To fill the gap in existing protection tools, there is a need for sophisticated scheme to offer sufficient security levels as well as increase awareness and knowledge of cyber risks/threats to users. Thus, a smart scheme with the aim of having fewer false positives and false negatives, and being less vulnerable to phishers' countermeasures by using the capabilities of artificial intelligence, is highly required. Intelligent capabilities may include classification, heuristics, and comparing objects via solidity algorithms, visual similarities and other machine-learning techniques that mainly depend on a detailed psychological investigation to study human perceptions and how users react to cyber-attacks. User requirements are the major factor in any protection system in terms of identifying the behaviour, motives, and drivers of cyber issues. In addition, system requirements are another important factor in providing quick online monitoring capabilities with less memory usage, speedy information retrieval and effective storage space. Protection tools are required to provide real-time monitoring support to various types of users and offer clear, intuitive explanations for the warnings they provide. In turn, users are able to respond effectively to security warnings. Effective training and educational support for users, with the main aim of engaging users in learning and education regarding cyber-attacks, should be provided by proposals to offer a high level of accuracy, as users will be aware of implicit and explicit cyber risks/threats.

V. Conclusions

Internet users face thousands of cyber-attacks every day because of the increasing reliance of users on website communications, emails and numerous 'anytime, anywhere' technology solutions. An intelligence tool that adequately understands cyber-attack mechanisms and users' behaviours in terms of assumptions, decision-making and reactions to cyber threats/risks is still missing. In this paper, the state of the art of the cyber security field of study and its importance in everyday online activities is investigated. It provides a useful cyber-attack taxonomy and classification that helps users involve themselves in a protection process to identify attacks and measures for cyber security. Existing protection systems which target cyber threats and risks are evaluated against three of our criteria for an effective anti-cyber-crime system: resilience to cyber attacks' countermeasures; real-time support and needs-based action; training and educational materials to increase users' awareness of cybercrimes. This evaluation and review of the existing attacks and tools will help researchers in the cyber security field of study to propose useful and effective protection schemes for current and upcoming attacks.

References

[1] Symantec, "Internet Security Threat Report," 2016. [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

[2] InfoSec, "Phishing Tools & Techniques," 2016. [Online]. Available: http://resources.infosecinstitute.com/category/enterprise/phishing/phishing-tools-techniques/.

[3] McAfee, "McAfee Labs Threats Report," 2015. Available: http://www.mcafee.com/uk/resources/reports/rp-quarterly-threats-aug-2015.pdf.

[4] M. Evans, L. A. Maglaras, Y. He, and H. Janicke, "Human Behaviour as an aspect of Cyber Security Assurance." Evans, Mark, et al. "Human Behaviour as an aspect of Cyber Security Assurance." arXiv preprint arXiv:1601.03921, 2016.

[5] D. John E, "Data breaches in UK healthcare sector double since 2013, ICO numbers show | Security | Computerworld UK." [Online]. Available: http://www.computerworlduk.com/security/data-breaches-in-uk-healthcare-sector-double-since-2013-ico-numbers-show-3589814/.

[6] A. B. Shahri, Z. Ismail, N. Zairah, and A. Rahim, "Security Effectiveness in Health Information System: Through Improving the Human Factors by Education and Training," Aust. J. Basic Appl. Sci., vol. 6, no. 12, pp. 226–233, 2012.

[7] PhishTank, "PhishTank Site Checker." [Online]. Available: https://addons.mozilla.org/en-GB/firefox/addon/phishtank-sitechecker.

[8] Google, "Google Safe Browsing." [Online]. Available: https://developers.google.com/safe-browsing.

[9] Y. Zhang, J. Hong, and L. Cranor, "CANTINA: A Content-Based Approach to Detecting Phishing Web Sites." In Proceedings of the

16th international conference on World Wide Web, pp. 639-648. ACM, 2007.

[10] M. Dunlop, S. Groat, and D. Shelly, "GoldPhish: Using images for content-based phishing analysis," in 5th International Conference on Internet Monitoring and Protection, ICIMP 2010, 2010, pp. 123–128.

[11] C. Simmons, C. Ellis, S. Shiva, D. Dasgupta, and Q. Wu, "AVOIDIT: A cyber attack taxonomy," 2009.

[12] T. Takada and K. Amako, "A Visual Approach to Detecting Drive-by Download Attacks." In Proceedings of the 8th International Symposium on Visual Information Communication and Interaction, pp. 162-163. ACM, 2015.

[13] N. Abdelhamid, A. Ayesh, and F. Thabtah, "Phishing detection based Associative Classification data mining," Expert Syst. Appl., vol. 41, no. 13, pp. 5948–5959, 2014.

[14] M. A. Faysel and S. S. Haque, "Towards Cyber Defense: Research in Intrusion Detection and Intrusion Prevention Systems," IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 10, no. 7, 2010.

[15] C. Song, J. Zhuge, X. Han, and Z. Ye, "Preventing Drive-by Download via Inter-Module Communication Monitoring." In Proceedings of the 5th ACM symposium on information, computer and communications security, pp. 124-134. ACM, 2010.

[16] M. Kjaerland, "A taxonomy and comparison of computer security incidents from the commercial and government sectors," Comput. Secur., vol. 25, no. 7, pp. 522–538, 2006.

[17] C. Tucker and T. Donlea, "Top 9 Fraud Attacks and Winning Mitigating Strategies." [Online]. Available: https://www.cybersource.com/content/dam/cybersource/CyberSource_MRC_Survey_Top_9_Fraud_Attacks.pdf.

[18] M. Uma and G. Padmavathi, "A Survey on Various Cyber Attacks and their Classification.," IJ Netw. Secur., 2013.

[19] "Cyber Security Information Sharing Act of 2015." [Online]. Available: https://www.congress.gov/bill/114th-congress/senate-bill/754

[20] "The UK Cyber Security Strategy Protecting and promoting the UK in a digital world." [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

[21] "Budapest Convention of Cybercrime." [Online]. Available: http://www.coe.int/en/web/conventions/.

[22] "Be Cyber Streetwise." [Online]. Available: https://www.police.uk/news/be-cyber-streetwise-three-simple-steps/.

[23] "Making the UK a safer place to do business and preventing cyber crime." [Online]. Available: https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security.

[24] A. Le Compte, D. Elizondo, and T. Watson, "A renewed approach to serious games for cyber security," in 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace, pp. 203–216, 2015.

[25] McAfee, "McAfee LiveSafe." [Online]. Available: https://www.mcafee.com/consumer/en-us/store/m0/catalog/mls_430/mcafee-livesafe.html?pkgid=430.

[26] A. Ferreira and G. Lenzini, "An analysis of social engineering principles in effective phishing," in 2015 Workshop on Socio-Technical Aspects in Security and Trust, pp. 9–16, 2015.

[27] "Google Chrome Privacy Whitepaper." [Online]. Available: https://www.google.com/chrome/browser/privacy/whitepaper.html.

[28] T. Gerbet, A. Kumar, and C. Lauradoux, "A Privacy Analysis of Google and Yandex Safe Browsing." PhD diss., INRIA, 2015.

[29] N. Virvilis, A. Mylonas, N. Tsalis, and D. Gritzalis, "Security Busters: Web browser security vs. rogue sites," Comput. Secur., vol. 52, pp. 90–105, 2015.

[30] P. Prakash, M. Kumar, R. R. Kompella, and M. Gupta, "PhishNet: Predictive Blacklisting to Detect Phishing Attacks," in 2010 Proceedings IEEE INFOCOM, pp. 1–5, 2010.

[31] Phishing Initiative, "European Union anti-Phishing Initiative," 2015. [Online]. Available: http://arche.depotoi.re/autoblogs/lamaredugoffrblog_6aa4265372739b936776738439d4ddb430f5fa2e/media/8fcc36eb.EN_EU-PI_FR_report-S1.pdf.

[32] N. Teraguchi and D. Mitchell, "Client-side defense against web-based identity theft," 11th Annu. Netw. Distrib., 2004.

[33] Mozilla, "Mozilla Thunderbird." [Online]. Available: http://www.mozilla.com/en-US/thunderbird.

[34] P. Lin, P. Lin, P. Chiou, and C. Liu, "Detecting spamming activities by network monitoring with Bloom filters," In Advanced Communication Technology (ICACT), 2013 15th International Conference on, pp. 163-168. IEEE, 2013.

[35] M. Aburrous, M. A. Hossain, K. Dahal, and F. Thabtah, "Intelligent phishing detection system for e-banking using fuzzy data mining," Expert Syst. Appl., vol. 37, no. 12, pp. 7913–7921, 2010.

[36] P. A. Barraclough, M. A. Hossain, M. A. Tahir, G. Sexton, and N. Aslam, "Intelligent phishing detection and protection scheme for online transactions," Expert Syst. Appl., vol. 40, no. 11, pp. 4697–4706, 2013.

[37] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "Anti-Phishing Phil," in Proceedings of the 3rd symposium on Usable privacy and security - SOUPS '07, p. 88, 2007.

[38] Centre for Information Systems Security Studies and Research (CISR), "Incorporating CyberCIEGE into an Introductory Cyber Security Course." [Online]. Available: http://cisr.nps.edu/cyberciege/CyberCIEGE Syllabus.html.

[39] Big Ambition, "Secure Futures." [Online]. Available: http://www.bigambition.co.uk/securefutures.

[40] APWG, "Phishing education landing page program." [Online]. Available: http://phish-education.apwg.org.