ISSN No:-2456-2165

End-User Awareness and Training

A Vital First Step for Cybersecurity

Mohammed Farik
Department of Computer Science and Mathematics
The University of Fiji
Saweni, Fiji

Abstract:- As cybercrime is one the rise, it is vital that all Internet users attain cybersecurity awareness and training, and make themselves unassailable. Hence, this paper first explains why it is vital for every Internet user to attain awareness and training in cybersecurity, then explains the training objectives to attain, and finally explains how to attain such awareness and training.

Keywords:- *Attacks; Awareness and Training; Cybersecurity; Threats; Vulnerabilities.*

I. INTRODUCTION

According to the ancient Chinese General Sun Tzu, an army that is better prepared, that is highly trained, that fights an unprepared enemy, and that makes no mistakes – is destined to win. [1]

Sun Tzu said, "Rely not on the likelihood of the enemy not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable." [1]

Moreover, he said, "being skillful in attack means that the enemy does not know what to defend and being skillful in defense means that the enemy does not know what to attack." [1]

Thus, to win any war, one needs to become unassailable, and to be that, one needs to undergo awareness and training to acquire the necessary skills.

Likewise, the cyberspace (better known as the Internet) is a digital warzone, that we find ourselves in. To defend ourselves on the internet, we need cybersecurity awareness and training.

As you know, the Internet is a powerful vehicle for many services that benefit humanity. Social networking, emailing, remote working, online studies, e-shopping, and Internet banking activities such as bill payment and mobile top-up are some of the most common activities that people in Fiji use the Internet for. However, the Internet is also a Pandora's box [2] through which hackers target the confidentiality, integrity, and availability of an internet user's data and other resources. Cybersecurity is the layers of defense that will support you in the battle against all evils of the Internet.

Thus, this paper is an attempt to create awareness on the need for cybersecurity awareness and training for every Internet user, with an outline on the content to train for, and a listing of how to achieve such awareness and training.

II. CYBER ATTACKS AND THREATS

According to Webscale Global E-Commerce Security Report 2021, cybercrime activities such as bad bots (malware), distributed denial of service, credit card skimming, credit card fraud, SQL injections, account takeover, and magecart attacks are on the rise [3]. Likewise, according to the CTM360 Cyber Forecast for 2021, there can be more hacking, malware, phishing attacks, and the resulting annual damages might increase to $6 trillion globally [4]. Also, look at Fig.1. that shows live botnet attacks that I captured via Looking Glass [5] over 4-days (29/7/21 – 02/8/21). Fig.1. registered 1.376 million live attacks by 10 botnets spanning 191 countries. These trends and statistics prove that the Internet is currently a very dangerous place.

Making matters worse, is the fact that during Covid-19 pandemic, students and employees are carrying out their responsibilities online from home. Inherently, the security layers through which their communications traverse may not be as ideal as those that are implemented on-site by the IT Services departments of Universities and Corporate bodies. Thus, if people are using their personal devices, via home Wi-Fi networks, there is a greater need to ensure that their devices as well as online activities through the private or public network are cybersafe.

It is important to realize that a network is only as strong as the weakest link. Note, just like war, in cyberspace, if an opponent is not skillful in defense, just one attack may be enough to break the first line of defense, allowing the enemy into the network.

For example, an unsuspecting user can easily fall victim to a phishing attack by clicking on an email link that has been crafted by a hacker to fetch identity information. This information can then be used as a pivot to create fake identify, create fake email account, create fake social media accounts, attack the user's bank account, and lure other people from the user's contact list. Also, in order to survive, a defender will need to successfully defend against all the attacks. It is therefore vital that not only IT Support people, but all internet users must undergo cybersecurity awareness and training.

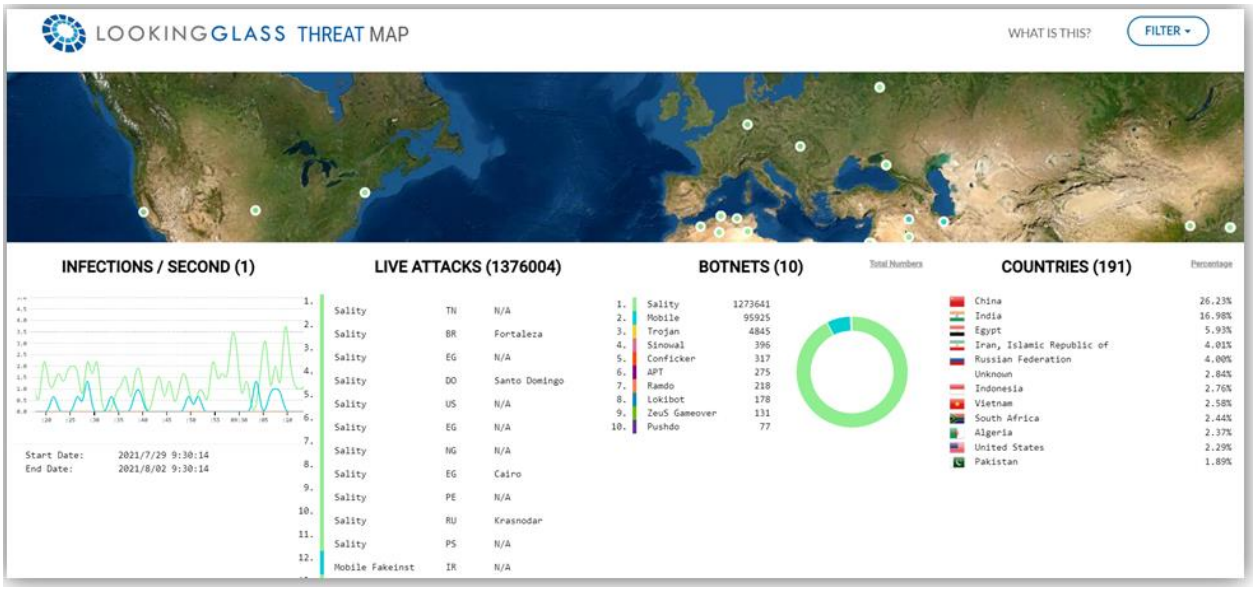

Fig. 1. Looking Glass Threat Map

III. CYBERSECURITY TRAINING OBJECTIVES

Specifically, cybersecurity awareness and training program must prepare common Internet users to be able to:

A. Understand Current Attacks and Threats

An internet user must understand the type of threats and attacks that one needs to defend against and apply appropriate countermeasures. According to Sun Tzu in the Art of War, "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every battle gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." [6]

B. Perform Vulnerability Assessment

To be able to defend well, one needs to understand the current weaknesses in their computers in relation to known exploits and attacks. Vulnerability assessment tools such as Nessus [7] can assess a computer and network to generate reports [8] which will help one to identify and neutralize critical vulnerability before an invader can take advantage of the situation.

C. Identify and Configure Security Features of the Endpoint

To understand the built-in security features of the end-user hardware, software, data, network technologies, and their security settings, so that one can choose to implement ideal security solutions and configure each setting appropriately. Knowledge on security features is also important in purchasing ideal hardware model and software version & build for use.

D. Select Third-Party Vendor Security Solutions

To understand and assess whether there is a need to install and configure any of the various types and alternative brands of third-party vendor's security solutions to protect an endpoint hardware, software, data, and network. Chances are that similar tool is already available built-in in the hardware, and operating system software. So, purchasing third-party software may just be an unnecessary expense.

E. Follow Ethical Principles, Organizational Policy, Industry Regulations, and Law

To understand the ethical, regulatory, and legal limits within which one should use an endpoint and its technologies. One should refrain from making any unethical decision, violating any policy, or being charged by police for any cybercrime offence, which can mean game over as far as one's professional career is concerned.

F. Practice Cybersecurity

Internet users must understand the safest way to carry out their common Internet activities and be able to recognize any anomaly to raise a red flag. Every click on the Internet must always be only after quick evaluation of the dangers that may be.

IV. AWARENESS AND TRAINING

With the right cybersecurity awareness and training, it is hoped that an Internet user should be able to defend against attacks, as well as make one's own Internet presence safer for others. However, because of the nature of Internet, information technologies, and cybersecurity field, awareness and training for the user is going to be a life-long process. One must learn new ways to defend as hackers learn new ways to attack, Today, end-users can attain cybersecurity awareness and training from the comfort of their homes by:

- Reading National Cyber Security Center (NCSC) infographics on cybersecurity issues [9].
- Viewing security videos on YouTube by TEDx Talks [10]
- Reading cybersecurity newsletters such as Station X - Threat Intelligence Update [11], SANS NewsBites [12], and SANS @RISK The Consensus Security Vulnerability Alert [13].
- Reading cybersecurity articles on technology vendor websites of Samsung [14], Android [15] Apple [16] [17], HP [18], Dell [19], and Microsoft [20].
- Reading organizational policies such as Acceptable Use Policy (AUP), ICT Policy, and Cybersecurity Policy.

- Understanding national laws such as Cybercrime Act 2021 [21], Online Safety Act 2018 [22], and the Computer Offences Sections 340-346 in Crimes Decree 2009 [23].
- Participating in online webinars, seminars, workshops, and conferences which are organised by IT industry giants such as Institute of Electrical and Electronic Engineers (IEEE) [24], IBM [25], Google [26], and Microsoft [27].
- Reading cybersecurity articles published by open-access, and online journals
- Becoming a member and reading news and periodicals from professional organizations such as IEEE Cyber Security [28], IEEE Spectrum [29], IEEE Computer Society [30], IT Professionals New Zealand (ITP) [31].
- Completing online short courses offered via platforms such as Udemy [32], and Coursera [33].
- Completing an online compulsory university-wide ICT course with strong cybersecurity content.
- Completing an online undergraduate, or postgraduate major or specialization in cybersecurity [34].
- Completing an online training and industry certification such as CompTIA's Security+, CySA+, PenTest+, and CASP+ [35].

V. CONCLUSION

In conclusion, to be able to defend appropriately against cyber-attacks, awareness and training in cybersecurity is a vital first step, but a never-ending journey.

REFERENCES

[1]. L. Giles, Sun Tzu on the Art of War: The Oldest Military Treatise in the World, Leicester: Allandale Online Publishing, 2000.
[2]. N. S. Gill, "Understanding the Significance of Pandora's Box," 29 June 2019. [Online]. Available: https://www.thoughtco.com/what-was-pandoras-box-118577. [Accessed 5 September 2021].
[3]. Webscale, February 2021. [Online]. Available: https://www.webscale.com/wp-content/uploads/2021/02/Global-Ecommerce-Security-Report-2021.pdf.
[4]. CTM360, 2021. [Online]. Available: https://beta.ctm360.com/images/CYBER-THREAT-LANDSCAPE-2021.pdf.
[5]. Looking Glass, "Threat Map," Looking Glass, July 2021. [Online]. Available: https://map.lookingglasscyber.com/. [Accessed 29-30 July 2021].
[6]. L. Giles, Sun Tzu on the Art of War, Leicester: Allandale Online Publishing, 2000.
[7]. Tenable, "The Nessus Family," Tenable, 2021. [Online]. Available: https://www.tenable.com/products/nessus. [Accessed 4 September 2021].
[8]. C. Dumont, "Top Ten Vulnerabilities," Tanable, 5 April 2021. [Online]. Available: https://www.tenable.com/nessus-reports/top-ten-vulnerabilities. [Accessed 6 September 2021].
[9]. National Cyber Security Center, "Infographics at the NCSC," [Online]. Available: https://www.ncsc.gov.uk/information/infographics-ncsc. [Accessed 23 September 2021].
[10]. Youtube, "tedx talks security," [Online]. Available: https://www.youtube.com/results?search_query=tedx+talks+security. [Accessed 23 September 2021].
[11]. StationX, "Security & Privacy News and Alerts," [Online]. Available: https://www.stationx.net/research/security-alerts/. [Accessed 23 September 2021].
[12]. SANS, "NewsBites," [Online]. Available: https://www.sans.org/newsletters/newsbites/. [Accessed 23 September 2021].
[13]. SANS, "@RISK - The Consensus Security Vulnerability Alert," [Online]. Available: https://www.sans.org/newsletters/at-risk/xxi-18/. [Accessed 23 September 2021].
[14]. Samsung, "Samsung Newsroom U.S.," [Online]. Available: https://news.samsung.com/us/. [Accessed 23 September 2021].
[15]. Android, "Enterprise Security," [Online]. Available: https://www.android.com/enterprise/security/. [Accessed 23 September 2021].
[16]. Apple, "Privacy," [Online]. Available: https://www.apple.com/privacy/. [Accessed 23 September 2021].
[17]. Apple, "Newsroom," [Online]. Available: https://www.apple.com/newsroom/. [Accessed 23 September 2021].
[18]. HP, "Security Bulletins," [Online]. Available: https://support.hp.com/us-en/security-bulletins. [Accessed 23 September 2021].
[19]. Dell Technologies, "Newsroom," [Online]. Available: https://corporate.delltechnologies.com/en-us/newsroom.htm#/filter-on/Country:en-us. [Accessed 23 September 2021].
[20]. Microsoft, "Security," [Online]. Available: https://www.microsoft.com/en-us/security. [Accessed 23 `September 2021].
[21]. Government of Fiji, "Cybercrime Act 2021 (Act No. 3 of 2021)," [Online]. Available: https://laws.gov.fj/LawsAsMade#. [Accessed 22 February 2021].
[22]. Government of Fiji, "Online Safety Act 2018 (Act No. 8 of 2018)," [Online]. Available: https://laws.gov.fj/LawsAsMade#. [Accessed 22 February 2021].
[23]. Government of Fiji, "Crimes Decree 2009 (Decree no. 44 of 2009)," 5 November 2009. [Online]. Available: https://www.steptoe.com/images/content/2/3/v1/2393/3984.pdf. [Accessed 5 September 2021].
[24]. IEEE, "Conferences," [Online]. Available: https://www.ieee.org/conferences/index.html. [Accessed 23 September 2021].
[25]. IBM, "IBM Events," [Online]. Available: https://www.ibm.com/events/. [Accessed 23 September 2021].
[26]. Google, "Events," [Online]. Available: https://buildyourfuture.withgoogle.com/events/#!#view-all. [Accessed 23 September 2021].

[27]. Microsoft, "Research," [Online]. Available: https://www.microsoft.com/en-us/research/events-conferences/. [Accessed 23 September 2021].
[28]. IEEE Cyber Security, "Home," [Online]. Available: https://cybersecurity.ieee.org/. [Accessed 23 September 2021].
[29]. IEEE , "IEEE Spectrum," [Online]. Available: https://spectrum.ieee.org/. [Accessed 23 September 2021].
[30]. IEEE, "IEEE Computer Society," [Online]. Available: https://www.computer.org/. [Accessed 23 September 2021].
[31]. IT Professionals New Zealand, "About ITP," [Online]. Available: https://itp.nz/. [Accessed 23 September 2021].
[32]. Udemy, "Cyber Security Courses," [Online]. Available: https://www.udemy.com/topic/cyber-security/. [Accessed 23 September 2021].
[33]. Coursera, "Learn Without Limits," [Online]. Available: https://www.coursera.org/. [Accessed 23 September 2021].
[34]. G. Chokhonelidze, G. Basilaia, M. Kantaria and M. Dgebuadze, "Teaching the Cybersecurity Courses at the University in Georgia," International Journal of Innovative Science and Research Technology, vol. V, no. 4, pp. 648-651, 2020.
[35]. CompTIA, "CompTIA Certifications," [Online]. Available: https://www.comptia.org/certifications?level=cybersecurity. [Accessed 23 September 2021].