

Review of knowledge base according to Information Technology Safety Awareness

Anikó Szarvák
 Doctoral School of Applied Informatics and Applied
 Mathematics
 Óbuda University
 Budapest, Hungary
 szarvak.aniko@nik.uni-obuda.hu

Valéria Póser
 Institute of Biomaterials and Applied Artificial Intelligence (BMI)
 Óbuda University
 Budapest, Hungary
 poser.valeria@nik.uni-obuda.hu

Abstract— The majority of cyberattacks are targeting companies, government or service provider parties, but attacks and threats are not limited to these parties. Also, the most challenging in defense side to raise awareness of the employees, but these employees most of their time are people who are enjoys the benefits of technology and uses it in their private life. Recently, according to IT Security Technology evolution, from Information System perspective, the human is the weakest link. This is supported by increased Social Engineering activity due pandemic reasons. This paper reviews the recent attacks and techniques according to increased e-commerce, internet and mobile activity. The goal of this review is to highlight how the usage of Information Technology and Information Communication Technology changed and review the connected fields, specially, the change in human side. This review defines new ways to achieve safe and secure usage through Information Technology Safety Awareness beyond Company Policy driven Information Security Awareness which is predefined in NIST SP-800-50 in 2003. The NIST standard suggests awareness training where it blurs compliance with corporate policy and basic, user knowledge. This review points out is that blending Information Technology Safety Awareness is problematic and straightening it up is a possible way to make user insecurity less of a problem.

Keywords— Information Technology Safety Awareness, Information Communication Technology, human side

I. INTRODUCTION

Nowadays it is important to connect via Internet. Usage of PC-s, mobile handhelds and tablets are essential in personal life too, not only in work. Therefore, it is also important to be prepared personally for threats of Internet usage. In 20 years, communication technology has become an important part of our everyday lives. It stepped out from the boundaries of work. More research confirms that the velocity in the development of technology is not being followed by the human side at a sufficient speed.

Due the outstanding growth of e-commerce and mobile handheld activity, Europol [1] stated: “Criminal activities appropriating the COVID-19 outbreak have also gone mobile, with some instances of malware targeting Android devices.” In their warning on threats the areas such mobile usage, phishing, ransomware attacks are highlighted. We assume these areas are not only related to Covid-19 pandemic, but these threats are emerging in general according to private life Internet usage.

Mobile handheld device rise is undeniable. Guardian [2] stated in 2016, “PC sales have been in decline for years, while smartphones have reached at least 80% saturation within most

developed markets and have become the sole point of access to the internet for many in developing nations.”

In ENISA Threat Landscape 2020 - List of top 15 threats [3], Phishing is ranked as no. 3. In the report, ENISA states “Trend analysis of the phishing threat between January 2019 and April 2020. Phishing attacks ranked 3rd in the threat landscape, raising from the 4th position in 2018.” More interesting, in the detailed report [4] “667% increase in phishing scams in only 1 month during the COVID-19 pandemic”.

Phishing is just one of widely used Social Engineering (SE) attacks. In ENISA Threat Landscape, 5 of 15 threat is related to SE which means one third of the successful attacks are depends on human. These threats are the following:

- Malware,
- Phishing,
- SPAM,
- Identity theft,
- Ransomware.

Raising awareness is a must to reduce the risk of attacks. Instead of restricting the usage of the technology, users of the technology should be aware of the potential dangers, similar to driving car or using weapons. Importance of awareness is becoming more important as technology advances. Hence, as in physical life, the safeguards of IT are one step behind of it.

From various reports the tendency of cybercrime, both attack numbers and volume of loss increasing. According to the Internet Crime Complaint Center (IC3), there were U.S. \$1.3 billion in losses in 2018 due to Business Email Compromise (BEC) scams. [5]

Verizon’s 2018 Data Breach Investigations Report points out that email is the number one vector for both malware distribution (92.4 percent) and phishing (96 percent) stated by Cisco. [6] In Verizon’s 2020 Data Breach Investigation report points out that 22% of breaches involves Phishing as attack vector. [7]

In addition to the above collected reports and numbers, Purplesec [8] states “98% of cyberattacks rely on social engineering”. We assume, in most of the cases, only awareness, more precisely Information Technology Safety Awareness (ITSA) is the key defence tool what we – people – have. The knowledgebase of ITSA collects and summarizes the ways in which cybersecurity attacks can be detected for the average user and the possible ways to defend themselves.

II. REVIEW OF CHANGE IN INTERNET USAGE

In telecommunication history, GPRS, 2G and 3G technologies supported the rise of cell phones connected to internet. IBM Simon is defined as first smartphone, released in 1994., then other cell phone companies stepped to this market. Nowadays smartphone mobile devices appearance dated to 2007, while Apple introduced the first iPhone. This means the smartphone technology is quite young, only 27 (14) years old.

We have to admit, the usage of Information Technology (IT) and Information Communication Technology (ICT) is changed in this decade. If we look back in time, 20 years ago we saw youngsters in the street listening Walkman or elders reading newspapers printed to paper, while they are using public transportation. Nowadays if we look around, we see people mostly a mobile in their hand. They are using instant messaging services, social network services or reading news, emails through it. Mobile started to spread in 1980. The statistics made by Areppim [9] shows that only in 36 years the mobile penetration earned 100% of the population of the world, based on the number of subscriptions. We note, it may be more if we count with mobiles without subscriptions. For a usage estimation, we calculated a growth on forecast data of subscriptions.

TABLE I. GROWTH ON SUBSCRIPTIONS

Millions of subscriptions per year		
2016	2020	%
7 418	7828	105,53%

We made a comparison on Internet usage based on infographics on “What happened in a minute on internet 2016” [10] and in 2020 [11]. We collected the same service usage numbers published in 2016 and 2020 and calculated the change of it.

TABLE II. GROWTH IN INTERNET USAGE

Internet service	Change in internet usage		
	2016	2020	%
Netflix, hours watched	69 444	764 000	1100,17
Facebook logon events	701 389	1 300 000	185,35
Google search	2 400 000	4 100 000	170,83
Youtube video viewed	2 780 000	4 700 000	169,06
E-mail sent	150 000 000	190 000 000	126,67
Tinder swipes	972 222	1 600 000	164,57

The percentages of the service usage between 2016 and 2020 shows significant growth at the examined services. We found it is less affected by the growth of mobile penetration and most affected by the spread of internet availability, worldwide. We assume, Netflix growth is distorted, compared to others due the company’s expansion policy and pandemic effect. Therefore, relying on other service usage growth, we estimate an average 163,3% on 5 years basis which is significantly higher than growth of mobile subscription penetration, where we found only 105,53%.

If we compare the growth of mobile subscription and the estimated average growth of service usage we can conclude, the usage of services is not depending on the number of the mobile subscriptions. Also, we assume, the services, like

Youtube, Netflix, Facebook, Tinder and other services are mostly used outside of the workplace.

A. Cybersecurity treaths

The European Union Agency for Cybersecurity (ENISA) articulates in their research “List of top 15 threats” [12]: “During the next decade, cybersecurity risks will become harder to assess and interpret due to the growing complexity of the threat landscape, adversarial ecosystem and expansion of the attack surface.” We reviewed the listed threats according to the possible targets and have been made a classification whether these attacks are against companies or against people regardless of whether it may occur in connection with work or private life.

TABLE III. POSSIBLE TARGETS OF ATTACKS

Attack categories	Attack targets	
	Against Companies	Against People
Malware	x	x
Web based attacks	x	
Phishing	x	x
Web application attacks	x	
Spam	x	x
Distributed Denial of Service (DDOS)	x	
Identify theft	x	x
Data breach	x	
Insider threat	x	
Botnets	x	x
Physical manipulation, damage, theft and loss	x	x
Information leakage	x	x
Ransomware	x	x
Cyberespionage	x	x
Cryptojacking	x	x

This classification is based on the fact that the success of the attack requires assistance from user side. However, we admit, those people are more likely to be a target of an attack, who linked to key position at a company or in government, not only they are affected by for example identity theft. The table classifies the attack targets based on the assumptions above. According to the table, 10 of the ENISA’s top 15 attacks may targeting people who are not connected any companies, government. If we investigate the awareness from another perspective, people may not connect to any of Information Security Policies (ISP) maintained by companies, government, and they are not trained in Information Security Awareness too by companies or government.

These attacks are targeting people in their private life. Therefore, we assume the Security Awareness should not be relate only companies defined ISP. Security awareness should reach ICT users, generally. All of the users who has a personal computer, using mobile devices or wearables, accessing services via Internet must be educated against threats and attacks. We assume these fields are more related to general ICT usage instead of a company’s or government’s ISP and therefore the controls are not should be affected directly from an ISP rather it should be driven by ITSA, which addresses

private user's knowledge through tangible examples from their everyday life.

Since 2003, the NIST Special Publication 800-50 Building an Information Technology Security Awareness and Training Program [13] which is a fundamental document not only for federal agencies at United States of America but for IT security experts globally, a baseline standard for information security awareness trainings. This publication summarizes the areas that define the training topics, well thought out and comprehensive. But in the past 17 years, according to dramatic evolution in ICT, new threats showed up and cybersecurity threats become popular, natively against people, not only against companies or government or their stakeholders.

III. PROTOTYPE OF ITSA

The prototype of ITSA collects cybersecurity attack samples which are perceptible by anybody who uses mobile handhelds or PCs. The awareness training built up to measure individuals' awareness. This measuring process is used to present the progress of the audience and highlight the fields with lack of awareness.

The goal of any kind of awareness is to handle risks and support the state of security as defined by Muha [14] "closed, full, continuous and proportionate protection is provided". From Data Privacy perspective, for individual users the protection of their data can be described with state of security as well as companies' business data protection.

If we count the fact, average people face with cybersecurity threats via a small screen, ITSA must addresses the following end-user related fields with topics discussed:

- Network knowledge – trusted networks connection
Network knowledge area – trusted networks connection which is a key to build trust in the whole Internet. ITSA presents how easy to steal data through unencrypted connections, eavesdropping and man in the middle (MITM) attack. The goal with it to highlight the risk of untrusted network usage, for example free Wi-Fi services.
- Software knowledge area – Begin with the Software installation from non-secure source, across malicious code, spyware and trojans which are may installed with the permission of the user to PC or Mobiles, Tablets. The message for users is to be cautious with software downloaded from the Internet, specially from unknown source. Also, ITSA adds information on how to check software reliability and the permission handling of resources to the knowledgebase.
- Resource knowledge – ITSA collects privacy and security topics according to application installation and permission settings. Nowadays highlighted attack is the ransomware. In this area illustrated these kinds of attacks with use-cases in connection with fields of network, e-mail, WWW and Social Network. From Mobile perspective, banking malwares or other malicious code described in PC are relevant threats are presented here.
- Internet resource knowledge, such E-mail, World Wide Web (WWW) and Social Network (SN) usage – in this area ITSA highlights Phishing, SPAM and infected attachments which are key figures of an

attack. The main focus is on how many threat actors targeting and what are the most common points of an attack. Also, in this area, ITSA focusing on privacy considerations, threats on information share, visibility on web. In this area ITSA illustrates attacks with use-cases in connection with fields of network, e-mail, WWW and Social Network.

- Authentication credentials area – This section in ITSA contains the common problems of password weaknesses and draws attention on multi factor authentication topics. We address the same credential usage of multiple resources. This area presents risk according to same credential usage. Additionally, this area addresses weak credentials which is ease the attacker to access our data via e-mail, WWW or Social Network.

We reviewed the assets and services which are average users uses on daily basis. During the collection of ITSA knowledge base, we added the general SE related threats to end-user related fields. The collection of knowledge base points is showing use-cases in area to affected fields. With this matrix we defined five area to transfer knowledge on recent attacks. In ITSA we focus on why an end-user should be cautious and what an end-user can do to prevent an attack. Through all the cases we present the audience, we are going to strengthen them, they are able to do effective steps for their secure state.

ITSA addresses nearly the same topics which are addressed by ISA trainings based on ISP. The main difference is these ITSA trainings focus on how to do instead of company safety measures.

We note, the ISP's contains special use-cases and controls shaped to the company, therefore ISP based ISA is likely focus on what to do and what not to do. This kind of awareness trainings' goal is to direct the employee's behaviour. To achieve it they focus on the mitigation which is required by the company's IT security. The outcome is the attendees are familiar with cybersecurity terms. This is underpinned by a Pew Research Center survey [15] finds that Americans' understanding of technology-related issues varies greatly depending on the topic, term or concept. The majority of U.S. adults can correctly answer questions about phishing scams or website cookies. We assume these trainings are fails in long term because they affect the knowledge and the behaviour but not affects the attitude.

In contrast, the ITSA addressing the attitude. Through real life examples in connection with physical world can affect the attitude too. It is supported by the fact that people are touched with ransomware communication which connected to real-life ransom situation. It is usually phrased that Social Engineering (SE) attacks are addressing human weaknesses, such sympathy, helpfulness or cooperation, also these attacks are addressing naivety. If ITSA addresses attitude-change, we can also use the same human reactions, such sympathy, helpfulness and cooperation as strengths. Also, naivety can be addressed by attack operation examples which are illustrated by physical life attempts. ITSA presents cyberattack types connected to real-life actions; therefore, it is tangible for the audience.

All of the presented threats are described with physical life examples which are triggers defence reaction on the human side. We achieved good results before in similar case: "In a

case when we sent out a newsletter about ransomware and its capabilities of destruction flavoured emotionally, we got feedbacks from our end-users, full of understand of the risk and caution – awareness – on the topic. They highlighted they are touched by the message and they are felt the situation. The message sounded like this: “You can see kidnappings in movies [...] Imagine this could happen, kidnapping pictures of your loved ones, your family, from your computer.” [16]

We assume if end-users usually are not knowing what is happening behind the screen while using internet, reaching a website or using an application on mobile and what can happen while they are using it, they cannot be aware. Also, there is a common belief on personal computers and handhelds that if no one touches them, it does nothing. Based on these common believes, the ITSA focuses on the attitude but also includes two separate fields, the knowledgebase and the measuring process.

We agree the finding formulated by Bada et al. “The fact today is that security awareness as conceived is not working. Naturally, an individual that is faced with so many ambiguous warnings and complicated advice, may be tempted to abandon all efforts for protection, and not worry about any danger.” [17] This opened to us a new direction on ITSA development.

A. ITSA knowledgebase

“People know the answer to awareness questions, but they do not act accordingly to their real life” and “Simple transfer of knowledge about good practices in security is far from enough.” [18]. We agree with these findings, also we assume presenting the operation principles of specific attack is helpful. Knowing how an attack works can ease better understanding. Through this kind of knowledge transfer, we assume, we are able to raise knowledge on risk which may indicate better awareness through change in attitude.

“There is a need to separate ISP based ISA from the overall basic Information Technology Security Awareness. An independent definition of Information Technology Safety Awareness is knowledge or perception of a situation or a fact in Information Technology field or related area.” [16]

Additionally, ITSA is addresses risks through illustrative examples to connect ICT threats to real-life use-cases. This is necessary to bring closer these threats to the audience, make it concrete and tangible. This eliminates the shortcomings of most awareness training as described by Stewart et al.: “For information security awareness techniques to improve in effectiveness and efficiency it is clear that information security awareness content can’t be created from what the technical experts want to tell people, the contents of a technical standard or the prevailing best practice topics but rather the audience themselves that it seeks to influence and protect.” [19]

The goal is not to threaten the audience. This is supported by studies like Bada et al.’s article about cybersecurity awareness: “Threatening or intimidating security messages are not particularly effective, especially because they increase stress to such an extent that the individual may even be repulsed or deny the existence of the need for any security decision.” [17]

Beside the ITSA knowledgebase quite important to achieve behaviour change. Regular knowledge share scenarios are failing in some circumstances. Therefore, ITSA knowledge share follows a method, that links cybersecurity

threats with physical life conditions. The goal of ITSA is to connect cybersecurity threats to real-life risk and provoke defence reaction. ITSA is can be used by wide audience, anybody who have access internet, using PC or Mobile. ITSA implements an awareness training connecting ICT related threats to real-life risks to address defence reactions helps to change attitude instead of addressing knowledgebase or changing behaviour. Also, ITSA is applicable widely, from primary school, thus children are also affected by cyberattacks.

B. Measuring progress

The goal with this prototype of ITSA is to raise awareness with easily understandable examples. Therefore, during the awareness education, measuring the progress of the end-user side is indispensable. The measurement of the process has two separate questionnaires. To the attendees before and after the training the same image-based questions asked. The questionnaire not measuring the knowledgebase. The goal is to measure the change in the emotional reaction and the consciously or unconsciously reaction. The image-based questions illustrate the threats which are visible by average end-users.

In the questionnaire the images are not labelled. This is essential, because we want the end-users to react without any additional information, as it should happen in a real situation. In this case they are not influenced and not diverted in the direction of any reaction. They are on their own as it is usually the case when using ICT services. In addition to summarizing security awareness topics, ITSA aims to measure and address gaps based on measurement immediately for the audience. The goal with the measuring process is twofold. First, the audience get immediate feedback on their current state of awareness progress. Second, the level of security awareness of a group can be determined on the basis of aggregation. Based on these aggregated results targeted practices can be introduced to further raise of awareness.

C. Audience of ITSA

ITSA addresses general knowledgebase therefore, the threats may affect anybody who is connected once the internet, using mobile, applications, loading sites from world wide web, using Social Network sites and e-mails. Audience of ITSA can be anybody. The use-cases defined in ITSA is easily understandable and usable by end-users.

IV. CONCLUSION

Awareness training topics suggested by NIST-SP 800-50 in 2003 are relevant today, however the environment is changed. The rise of ICT, PC and Mobile spread and wide usage escalated the cyberattacks too and the weakest link is defined as the people who are using it. Nowadays accessing internet is not a company related privilege, it is natively available for near anybody. In former time, while internet usage was only available through workplace, directing employees with ISP was relatively easy. Today, internet users are not prepared exactly the cyberattacks and their attempts are usually not directed by ISP or ISA.

Raising awareness is a must to reduce the risk and impact of cyberattacks. Instead of restricting the use of the technology, end-users of the technology should be aware of the potential dangers, similar to driving car or using weapons. Importance of awareness is becoming more important as technology advances hence, as in physical life, the safeguards

are one step behind of it. In this situation, risk reduction can be achieved by increasing security awareness.

ITSA topics collected and organized for average end-users. The collected and presented attack types are demonstrating the key points which are detectable by end-users. While it is connected to real life examples, direct emotional reaction may occur. This supported by the measuring process which gives direct feedback to the audience on their progress.

ITSA follows a knowledge share method where cybersecurity threats are linked with physical life events. Measurement process uses the appearance of possible cybersecurity attacks to collect the audience reactions and presents the results immediately for the audience.

ACKNOWLEDGMENT

Authors gratefully acknowledges the support of the Doctoral School of Applied Informatics and Applied Mathematics on this research.

REFERENCES

- [1] Europol Covid-19: Mobile Threats
<https://www.europol.europa.eu/covid-19/covid-19-mobile-threats>
Accessed: 2021. 05. 20.
- [2] Mobile web browsing overtakes desktop for the first time.
<https://www.theguardian.com/technology/2016/nov/02/mobile-web-browsing-desktop-smartphones-tablets> 2016. Accessed: 2021. 05. 20.
- [3] <https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic> Accessed: 2021. 05. 20.
- [4] <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl2020-phishing> Accessed: 2021. 05. 20.
- [5] https://www.ic3.gov/Media/PDF/AnnualReport/2018_IC3Report.pdf
Accessed: 2021. 05. 22.
- [6] <https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/email-threat-report.pdf> Accessed: 2021. 05. 22.
- [7] J. Dolan: Psychology in Phising, IASP 470 Security System Capstone, 2017.
- [8] <https://purplesec.us/resources/cyber-security-statistics/#SocialEngineering> Accessed: 2021. 05. 25.
- [9] https://stats.areppim.com/stats/stats_mobilexpenetr.htm Accessed: 2021. 09. 12.
- [10] <https://www.visualcapitalist.com/what-happens-internet-minute-2016/>
Accessed: 2021. 09. 12.
- [11] <https://themarketingintrovert.com/content-marketing/internet-minute/>
Accessed: 2021. 09. 12.
- [12] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-list-of-top-15-threats/at_download/fullReport Accessed: 2021. 03. 05.
- [13] National Institute of Standards and Technology - NIST: Building an Information Technology Security Awareness and Training Program. Wilson, M. and Hash, J. Computer Security Division Information Technology Laboratory. October 2003.
<http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf>
- [14] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, 2008 [In.: Bolyai Szemle, XVII. évf. 4. szám, p.137-156., Budapest: ZMNE BJKMK, ISSN: 1416-1443]
- [15] M. Anderson and E. Vogels, "Americans and digital knowledge," Pew Res. Center, Washington, DC, USA, Tech. Rep., 2019. [Online].
<https://www.pewresearch.org/internet/2019/10/09/americans-and-digital-knowledge/> Accessed: 2021. 05. 20.
- [16] A. Szarvák, V. Póser: Information Technology Safety Awareness – a review of regularly used terms and methods, AIS 2020, 15th International Symposium on Applied Informatics and Related Areas organized in the frame of Hungarian Science Festival 2020 by Óbuda University, 2020, pp. 107-111., ISBN 978-963-449-209-2
- [17] Maria Bada, Angela M.Sasse and Jason R. C. Nurse: Cyber Security Awareness Campaigns: Why do they fail to change behaviour?
- [18] Information Security Forum (ISF): From Promoting Awareness to Embedding Behaviours, Secure by choice not by chance, February 2014. <https://www.securityforum.org/shop/p-71-170>
- [19] Stewart, Geordie; Lacey, David: Death by a thousand facts: Criticising the technocratic approach to information security awareness, Information Management & Computer Security, Volume 20, Number 1, 2012, pp. 29-38(10) ISSN: 0968-5227