frontiers in Computer Science

ORIGINAL RESEARCH
published: 17 September 2020
doi: 10.3389/fcomp.2020.00025

Handling User-Oriented Cyber-Attacks: STRIM, a User-Based Security Training Model

Aymen Hamoud[1,2]* *and Esma Aïmeur*[1]*

[1] Department of Informatics and Operational Research, University of Montreal, Montreal, QC, Canada, [2] Laboratoire d'Informatique REpartie (LIRE) Laboratory, University of Constantine 2 Abdelhamid Mehri, Constantine, Algeria

Privacy is an increasingly rare commodity. Once personal information is entered into a social network, it is no longer private. Such networks have become an incubation environment and carrier for cyber-attacks either by providing the necessary information about victims or facilitating the ways in which cyber-criminals can reach them. Social media create relationships and trust between individuals, but there is often no authority checking and validating user identities. This paper analyses different attack vectors examining the techniques used against end-users, who are targeted as a way of accessing larger organizations. It shows how the information that is disclosed to social networks can be transformed to provide insights about an organization, and the role of the victim in this process. These leaks not only expose users to the risk of cyber-attacks, but they also give attackers the opportunity to create personalized strategies that are difficult to avoid. This paper highlights these user-oriented attacks by first demonstrating the impact of disclosed information in the process of formulating an attack, in addition to group influence on an individual's vulnerability. Next, the various psychological manipulation factors and cognitive bias behind the user's failure to detect these attacks is demonstrated. This research introduces a theoretical user-based security training model called STRIM, which aims to educate and train users to detect, avoid, and report cyber-attacks in which they are the primary target. The proposed model is a solution to help organizations establish security-conscious behaviors among their employees.

Keywords: cyber threats, human behavior, privacy, security awareness, security training, social engineering, tutoring platform user-oriented attacks

OPEN ACCESS

Edited by:
A. S. M. Kayes,
La Trobe University, Australia

Reviewed by:
Mohammad Jabed Morshed Chowdhury,
La Trobe University, Australia
Jonathan Bakdash,
United States Army Research Laboratory, United States
Shahriar Badsha,
University of Nevada, Reno, United States

***Correspondence:**
Aymen Hamoud
hamoudaymen@outlook.fr
Esma Aïmeur
aimeur@iro.umontreal.ca

Specialty section:
This article was submitted to Computer Security, a section of the journal Frontiers in Computer Science

Received: *07 April 2020*
Accepted: *19 June 2020*
Published: *17 September 2020*

Citation:
Hamoud A and Aïmeur E (2020) Handling User-Oriented Cyber-Attacks: STRIM, a User-Based Security Training Model. Front. Comput. Sci. 2:25. doi: 10.3389/fcomp.2020.00025

INTRODUCTION

Today, online users are surrounded by threats that may differ in their techniques and motivations, but that all share one common point: these cyber-threats are increasingly target end-users directly (Isaca, 2018). Security reports show that spear phishing (Duman et al., 2016) was the number one infection vector employed by 71% of organized cybercriminal groups in 2017, while 75% of businesses reported being a victim of spear-phishing in 2018 (Proofpoint, 2019). Nearly 7% of the global web requests analyzed by Symantec (2018) lead to malware infection, and one email out of a 100 contained a malicious attachment (Isaca, 2018). These studies show that humans are the greatest factor in vulnerability, and that they are targeted by hackers. The statistics published in a several studies (Isaca, 2018; Proofpoint, 2018; Symantec, 2018) indicate that due to this success, this

vector will continue to play a significant role in cyber-attacks. The key to this success resides in the hacker's ability to exploit psychological triggers to fool and manipulate their victims (Bezuidenhout et al., 2010). Moreover, recent massive data leaks from various social media platforms such as *Facebook, Twitter, Linkedin, Myspace*, and even dating applications and games could help hackers improve this approach (Rubell, 2018). The vast amount of personal information disclosed on social networks has also enabled the development of to websites like *Peoplefinders*, *Whitepages*, and *Pipl* which track available personal information. All of these elements provide hackers with the necessary background information to develop sophisticated cyber-attacks against defenseless users.

Social media platforms have created several new channels through which criminals can attack end-users (Rathore et al., 2017). The threats inside these platforms are diverse and range from unwanted spam and targeted advertising (Can and Kaya, 2016) to cyber-attacks that can cause tremendous damage. In 2013, a fake post published on an account owned by the Associated Press (AP) discussed explosions in the White House and managed to destroy $136 billion in equity market value in a few minutes (Ficher, 2013). The encryption giant, RSA has also been a victim of phishing attacks, which allowed some hackers to get valuable information about the company's SecurID two-factor authentication fobs (Chabrow, 2011). Many other companies have also been victims, such as Sony, Ubiquiti (Krebs, 2018), and Equifax (Fleishman, 2018). Yahoo remains one of the most high profile examples, after one of their engineers fell for a spear-phishing email and hackers gained access, compromising 3 billion accounts. All the credentials and information of these compromised Yahoo accounts were on sale on the black market (Bulakh and Gupta, 2015). Organizations are increasingly affected by the behavior of their employees. These incidents go to show that any organization, even those with excellent security, are at risk. The horrific magnitude of these attacks has pushed some industrialists to separate their sensitive assets from the network by disconnecting every control process from the internet (Berinato and Bochman, 2019). However, the interactive nature of the business conducted by most companies forces them to stay connected and exposed to these dangers.

Currently, most security efforts are focused on the improvement of digital system security. Vulnerabilities and technical exploits have always been of interest to security vendors and even researchers. This explains the rarity of approaches that addressing this technical vulnerability through models such as attack graphs, attack trees, and security metrics to resolve user-oriented attacks. This attitude has created a false perception among security practitioners and constrained protection within a narrow range that does not go beyond solving technical vulnerability problems.

This paper provides a comprehensive and complete overview of user-oriented attacks. It studies aspects of psychological manipulation and the related cognitive bias that affects users' reasoning, making them vulnerable to these attacks. It then examines the impact of the group on one's safety and proposes methods of measuring user vulnerability. This paper significantly extends understanding of this subject by including novel attack vectors such as social circle and circle of trust.

In addition, this research proposes a theoretical model for a user security training system entitled STRIM. It is a tutoring platform that is personalized according to the user's cognitive profile and security knowledge level. This model uses theoretical and practical tests through real hacking scenarios to evaluate whether the user is vulnerable or not. The learning process is based on continuous sessions to adapt the system to the users' progress over time. To the best of our knowledge, no other model uses hacking scenarios to validate the users' progress has been proposed to date.

The structure of this paper presents the background in section Background. Section Overview of the User-Oriented Attacks then provides a taxonomy of user-oriented attacks, showing the impact of the group on one's vulnerability in a social network. Our solution, that we should educate and train users on cybersecurity, is then discussed section Security Training Model: STRIM before we present conclusions in section Conclusions.

BACKGROUND

Many prior studies discuss cyber-attacks, security awareness, and threat modeling in general, but only a few have gone beyond the technical context to examine the relationship between the information made available on social networks, and sophisticated attacks against vulnerable users. This section introduces user-oriented attacks and considers the effects user behaviors have on cybersecurity.

User-Oriented Cyber-Attacks

The last few years have seen increasing instances of social engineering attacks that manipulate traditional security vulnerabilities, and user-oriented attacks have become more effective and easier to carry out. The user has always been the weakest link in the security chain (Ghafir et al., 2018). This human factor is easily exploited through trust, sympathy, curiosity (Cialdini, 2001), and similar approaches that attempt to encourage users to click on malicious links, download, and install software, transfer funds, and much more (Proofpoint, 2018). Cyber threats are increasingly widespread. As Krombholz et al. (2015) have stated, social networks host these threats, either by providing sensitive information about users or providing an easy way to contact them (Sood and Enbody, 2013). Social networks are vulnerable to cyber threats because they create trusting relationships between individuals with no authority or parameters for checking and validating their identity (Zhang et al., 2017).

Aïmeur et al. (2013) have highlighted the main online data collection fields that threaten users and expose them to dangers such as privacy breach or identity theft. They explain various internet data collection techniques such as online data brokers, search engines, and background checks to show how these techniques are used to extract sensitive information about online users.

A survey conducted by the SANS Institute identifies the most frequent methods employed by attackers to launch cyber-attacks

on organizations. It found that drive-by downloads accounted for 48% of attacks. By exploiting web-based vulnerabilities (Neely, 2017), cyber threats are used as an entry point, enabling criminals to carry out more widespread attacks such as ransomware.

The more people reveal personal information (email addresses, job information, personal address, etc.), the more they are vulnerable. Heartfield and Loukas (2016) explain that people are defenseless after divulging their personal information through social media, and attackers know the structure of their passwords, as well as how to develop an effective social attack against them and their companies. Moreover, Rubell (2018) explained how hackers could turn fragments of publicly disclosed information into a useful picture about the organization, and the role of the target victim who works for that company. Bullée et al. (2018) have extracted different scenarios of social engineering attacks from books written by hackers, proving that psychological manipulation, such as the persuasion principles discussed by Cialdini (2001), are often used in interactions between the offender and the target in each attack.

In another study, Hadnagy and Fincher (2015) have discussed that the decision-making process is a sum of many factors, including emotions, perceptions, and even a user's physiological state. Moreover, they explain how influence principles such as reciprocity, obligation, and authority are used in the phishing process, to raise the level of the victim's fear, sadness, and anger, provoking an emotional response that means they do not use critical thinking in the encounter. Greene et al. (2018) set a web-based survey about three new phishing awareness training exercises, gathering qualitative and quantitative data, and analyzing the similarities and differences between clickers and non-clickers. The results show that the alignment of both the user context and the phishing message backdrop has a significant impact factor on phishing susceptibility, affecting individuals' depth of processing as well as their concerns about the consequences of their actions.

User's Behavior in Cybersecurity

Despite developments in technical security solutions, the human factor is always considered as the most vulnerable element of the security chain (Schneier, 2003). Vishwanath et al. (2011) explained how individuals tend to utilize heuristics or mental shortcuts, and judgment rules, to make quick inferences when they are presented with information online. Cialdini (2001) has also discussed the effect of cognitive bias on human behavior; he presented the essential traits that most people attach to "good thinking" as cognitive skills such as decision making and judgment. These abilities are crucial to real-world behavior, affecting the way people plan, judge risks and probabilities, evaluate serious evidence, and make effective decisions. More specifically, Lemay and Leblanc (2018) have discussed the subject of cognitive bias in cyber decision making, outlining that a high rate of false positive assertions can cause a confirmation bias, and that hindsight bias can further taint the effectiveness of the incident analysis process.

All people share specific influence patterns (Del Pozo et al., 2018). Social engineering is based on both security and psychological terms to take advantage of people's naivety. There are different motivators and incentives in people that make them susceptible to social engineering. Kotenko et al. (2011) have stated that the user's vulnerability is often associated with what they need (money, self-affirmation) or by emotional weakness (such as a desire for social approval, or self-esteem). As Heartfield and Loukas (2016) explain, cyber-attackers build upon these vulnerabilities using misdirection and manipulation to mislead the victim into performing a desired action. They also discuss the different deception techniques used by magicians and how these methods are used by hackers to circumvent human defenses.

Sasse et al. (2007) note that adopting safe behavior online is a three-step process that includes: security awareness, education, and training. Awareness campaigns aim to involve people's knowledge of cybersecurity by basing awareness on user perceptions of things which grab their attention. While security awareness education is important, in addition to training, the adoption of safe behavior also requires new models of thinking (Furman et al., 2011). Bain (2004) has argued that established mental models must be proven wrong before users accept and adopt new models. Indeed, one cannot convince users to adopt new online safe behaviors without proving to users that their behavior makes them vulnerable. However, adopting new security behavior is challenging, given that the users must engage threats and understand the process of successfully identifying and addressing security issues (Ki-Aries and Faily, 2017). The users must then be motivated to apply safe behaviors and improve their perceptions of risks.

In examining the motivations that inform security behavior, an empirical quantitative study by Dinev and Hu (2007) examined user behaviors in 339 IT professionals and business school students. This research showed that fear and awareness motivate the adoption of protective technologies. These findings show the awareness of the intentions that affect individual behavior is higher in those with greater technical knowledge. Another study by Pfleeger et al. (2014) introduced a framework based on empirical validation of both moral foundations theory and habit formation that can be utilized to achieve a stronger security culture. Furnell and Rajendran (2012) have also proposed a model to understand the compliance behavior of a user, identifying six factors that influence security behavior, job characteristics, organizational factors, workplace interactions, real-life exposure, perceived benefits, and wider awareness.

Various causes can lead to the failure of security awareness campaigns. Bada et al. (2019) mention that awareness programs were often treated as simple questions to be answered and do not always lead to expected behaviors. Some approaches that rely on invoking fear to change behaviors were also proven ineffective (Ahluwalia, 2000). Other approaches resulted in a lack of motivation and ability to meet the unrealistic expectations which may arise from poorly designed security systems and policies (Bada et al., 2019). Attackers are more likely to target an information system at its weak points, which makes securing the weakest link critical (Schneier, 2003). The severity and frequency of cyber-attacks will continue to expand, and the scheme of these

attacks will just improve and become more sophisticated over time (Symantec, 2018). Indeed, lack of security knowledge and compliance among users will always be recognized as a major contributing factor (Proofpoint, 2018). This puts us under the obligation to improve and adapt user-centric solutions to meet today's security requirements, mitigate recent cyber-threats, and establish safe security behaviors.

In this section, we have discussed subjects related to our study, as well as the previous research published on these topics.

OVERVIEW OF THE USER-ORIENTED ATTACKS

This section presents different attack vectors that are used against end-users of social networks. It defines user-oriented attacks and highlights some cognitive aspects that affect the user's reasoning. More specifically, it studies the social attack vectors used against users and proposes methods to measure their vulnerability.

The Manipulation Aspects

Manipulation is very similar to influence, but it is generally described as a deceptive intention that serves the manipulator. A skilled attacker or social engineer seeks to better understand their victims, and to steer their choices to be consistent with their goals (Hadnagy and Fincher, 2015). The following section highlights aspects of manipulation and techniques used by hackers during cyber-attacks, describing how cognitive bias that makes users vulnerable to this kind of manipulation.

Impersonation is the main element of most cyber-attacks against users in social networks. This involves the assumption of another person's identity, usually as a means of gaining status or other advantages (Reznik, 2012). The hacker analyzes the victim's entourage to pick the best profile through which they can attack the victim. Aïmeur et al. (2012) have explained how social network profiles can be easily rebuilt from information disclosed on the internet. For instance, by impersonating one of the victim's close friends, a hacker is more likely to deceive them into downloading malicious software or encourage them to click on a malicious link.

Persuasion is a process that aims to affect or change a user's behavior toward ideas and/or events, by using certain patterns to convey information, feelings, or reasoning; This is usually achieved using influence techniques such as "liking," social proof, and authority (Cialdini, 2001). The use of social networks has made it incredibly easy for hackers to make initial contact with their victims, as well as to share malicious links with them, for instance, through the comments or the posts in the groups. The attacker follows the same page or subscribes to the same group as the victim and can see their interests and use this to approach them in a friendly way and hide malicious intention.

Misdirection is the user's vulnerability to being distracted in the face of a situation they cannot handle or understand. Hackers often hide their attacks in the form of everyday unharmful interactions (such as birthday notes, funny video links, work-related attachments, etc.).

The interactive nature of social networks has made it incredibly easy for hackers to interact with their victims and to easily trick them into revealing sensitive information and click malicious links through the combination of manipulation and cyber-attacks. These techniques are widely used in different ways by hackers, depending on the context and the type of cyber-attacks.

Common Types of User-Oriented Attacks

A user-oriented attack could be defined as a specific scheme of cyber-attacks in which the attacker searches for and targets the system's users, instead of directly attacking the system itself. This scheme is adopted for a variety of reasons, for example as a way of getting around firewalls and intrusion detection systems. Indeed, this kind of cyber-attack gives the attackers an easier way to get access to the target systems or sensitive assets such as databases, sensitive files, or even control processes in industrial enterprises.

In a user-oriented attack, as shown below in **Figure 1**, the attacker searches for and extracts sensitive information about the user, such as their email or personal address, social network profiles, or even information on their[1] closest and most vulnerable friends, to build an efficient attack. Once the user is compromised, the attacker takes full control of their machine, so they can use their access to the system to spread malware within the corporate network and retrieve sensitive data.

In the following section, the different techniques that attackers use to deliver their malware into the target system are discussed.

Spear phishing attack is a more specific type of phishing activity than simple phishing, where the same malicious email is sent to as many people as possible. Spear phishing is carefully designed to target a single victim. Hackers take their time to conduct a deep search on the target users and create messages that are more relevant and personal to them. For instance, they can create forged official documents that contain personal information. Spear phishing often comes in the form of pretexting or spoof emails that appear to be from legitimate sources (Hong, 2012), to gain the user's trust and to influence them to lower defenses and download attachments that load the malware into the user's system (Akbar, 2014). This kind of attack is less likely to be detected and very difficult to defend against.

Fake landing pages are phishing web pages that look exactly like the original ones. They are created by copying the source code (HTML/CSS) of the original page to fool inexperienced users into entering their personal information, credentials, or financial details. For example, Facebook and Twitter phishing pages, banking, and corporate phishing pages. Or as in drive-by downloads where the user is led to a fraudulent page where they are tempted to download malicious software as if it were a free program like anti-virus, music, and games.

Malware attacks are a type of cyber-attack that carry malware (trojans, ransomware, and spyware) into the victim's computer. Malware is a piece of harmful software that is designed to cause damage to the target computer (Niemelä et al., 2016), either by stealing and encrypting files or creating a backdoor for the hacker to control the victim's machine. The payload or the

[1] "He" refers to "he or she;" "His" refers to "his or her," when applicable.

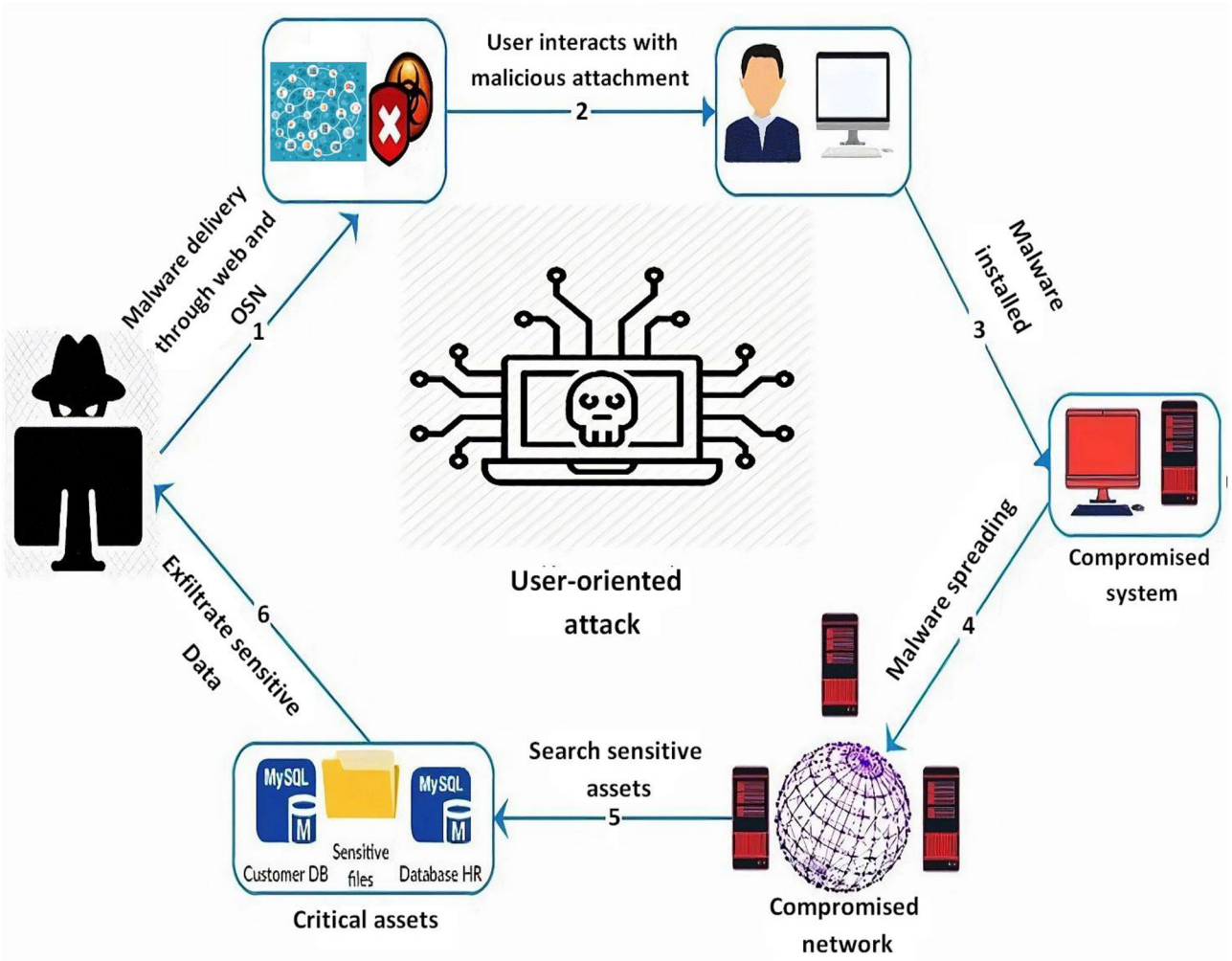

FIGURE 1 | The autopsy of a user-oriented attack.

download dropper methodology is often used in these attacks, where the first file is a small unharmful piece of code designed to evade detection and communicate with a command-and-control channel (Isaca, 2018) and the executable then receives commands to download malware which infects and compromises the host machine.

Man in the Middle and sniffing attacks target the home address, which is the most sensitive piece information. By hacking a victim's wireless router the attacker can easily perform different types of attacks. In man-in-the-middle attacks (MITM), the attacker intercepts and perhaps injects correspondence between two parties who believe they are directly communicating with each other (Adams, 2019). In sniffing attacks, the attacker captures network data packets to extract sensitive information (username, passwords, banking details).

Domain name server attacks involve hackers redirecting legitimate traffic to a malicious host by manipulating DNS entries. Malware on a system can tweak DNS entries in the host configuration file or use a DLL (Domain-link library) injection to redirect a browser to different domains.

Despite the manipulative approach and the sophisticated scheme of these cyber-attacks, the behavior of online users plays a major role in the success of these attacks. Indeed, there are many psychological factors that make users vulnerable to these types of manipulation.

The User's Vulnerability and Cognitive Bias

Research on decision behavior has shown that peoples' judgments and decisions are subject to many biases. They often rely on psychological methods known as mental shortcuts to make decisions. Although these shortcuts can accelerate the decision-making process, they can also lead to people making wrong choices and stereotypes.

The anchoring bias (also known as the Relativity Trap) is defined by the human tendency to rely heavily on the first piece of information they learn (Epley and Gilovich, 2001). In the case of impersonation, the victim user will always rely on the

false identity given to them by the hacker in treating subsequent information during the communication.

Confirmation bias is defined by peoples' affinity to favor information that confirms their previously held preconceptions (Plous, 1993). For instance, if the user builds a false perception of hacker identity (impersonation), the victim will build understanding on the interaction, based on this false information.

Courtesy bias is the tendency to give an opinion that is more socially correct than one's true beliefs to avoid offending others (Leon et al., 2007). In this instance the attacker shares information with users to push them to reciprocate and share information with the hacker.

The bandwagon effect describes people's desire to join a cause and be part of the crowd. It is a phenomenon in which people primarily do something because others do, regardless of their own beliefs (Leibenstein, 1950). The attacker claims to be conducting a report and cites indirectly other people from within the organization who have already participated. The report leads to a series of questions that manipulate the victim into revealing information about the systems and network (a type of operating system, network architecture, etc.).

The empathy gap is the tendency to underestimate the influence of feelings and emotions on behavior and decision making (Van Boven et al., 2013). Attackers often tend to evoke a victim's feelings (sympathy, praising), to push them into compliance.

Attentional bias is the affinity to pay attention to one thing while simultaneously ignoring others, which leads to failure in considering any other possibilities (Baron, 2008). For instance, the common idea that anti-viruses protect users against all threats on the internet leads them to ignore the possibility of being attacked.

Functional fixedness is the tendency to see objects as only working in one way, which leads to the failure of alternative solutions (German and Defeyter, 2000). For example, in spear-phishing scenarios, when legitimate-looking content leads users to fail to consider the risks of clicking on it.

Privacy Invasion and User Attack Vectors

In a highly interactive social network one's privacy not the only cause for concern. Many studies have looked at the effect of group dynamics on individual behavior, privacy, and vulnerability.

As represented in **Figure 2**, there are different vectors by which attacks against users can be carried.

Privacy and Multi-Party Privacy

Privacy-preserving can be defined as one's ability to decide who can see personal information and shared content on social networks. Privacy is not just about what one says or discloses; it is also what others say or disclose about that person (Such and Criado, 2018). For example, Jack does not like to share his picture nor location. Isabel takes a photo of Jack and herself and posts it on the social network. In this case, the information that Jack is trying to keep private is revealed against his will. Privacy disclosure is an aspect of risk that people face on social networks. Nowadays, hackers use the virtual entourage of the victim to create an effective attack.

Social Engineering and Manipulation

This is the use of deception, persuasion, and misdirection to engineer a false perception of the situation in the victim's mind and insinuate that the hacker as a reliable person or organization. The main goal of manipulating unsuspecting users is to fool them into breaking standard security procedures, either to gain access to the system or to obtain sensitive information (Del Pozo et al., 2018). For instance, personalized spear-phishing, tax, and bank scams, misplaced flash drives, phishing campaigns, etc.

Circle of Trust

Most users, even those who are security aware, have a trusted circle of people, a "circle of trust," with whom they have frequent digital interactions (exchanging USB drives, files, and emails) based on their ties and the implication of their needs, whether social or professional. Examples include the interaction between best friends, colleagues, student-professor, etc.

Acknowledgment, the digital trust circle, does not imply trust in real life, and reciprocity. For example, every user trusts their parents, but would be suspicious of an email coming from them if they do not have frequent digital interaction.

Social Circle

The social circle is defined as the one's digital entourage, the people with whom a user shares their virtual life, thoughts, and with whom they have limited regular interaction (e.g., Facebook friends, groups, followers, mail contacts, etc.). Users are more likely to open links and attachments if they are sent by friends.

Metrics to Define the User's Vulnerability

The vulnerability of any user is profoundly affected by their environment and the extent of their security knowledge of the users with whom they have frequent digital interaction with. If a user is compromised (hacked or infected by malware), the hacker can attack friends either by using their email or social profiles. Even the victim might unintentionally deliver malware while sending files on the internet.

The very interactive nature of social networks and development of sophisticated malware has transformed the concept of vulnerability. This is no longer a personal problem, as it also affects the victim's entourage. Indeed, being a victim of a cyber-attack exposes one's entourage to the same risks. For instance, the hacker can use the victim's email to send a malicious attachment to others and use a social profile to lead victim's network into clicking malicious links. In the following section, a series of metrics are proposed as a way of defining and measuring multi-party vulnerability.

Three degrees of risk were defined:

Vulnerable (**V**), *Highly vulnerable* (**HV**), and *Potentially compromised (PC)*.

Every degree of risk can be defined by one or many possibilities.

Remark: *Social network circle* (**SC**), *circle of trust* (**CT**), *Hacker* (**HK**), *Compromised user* (**CM**).

A vulnerable user **V** is a user with a low level of security knowledge and awareness, which puts them in danger of intentionally downloading malware or interacting with attackers.

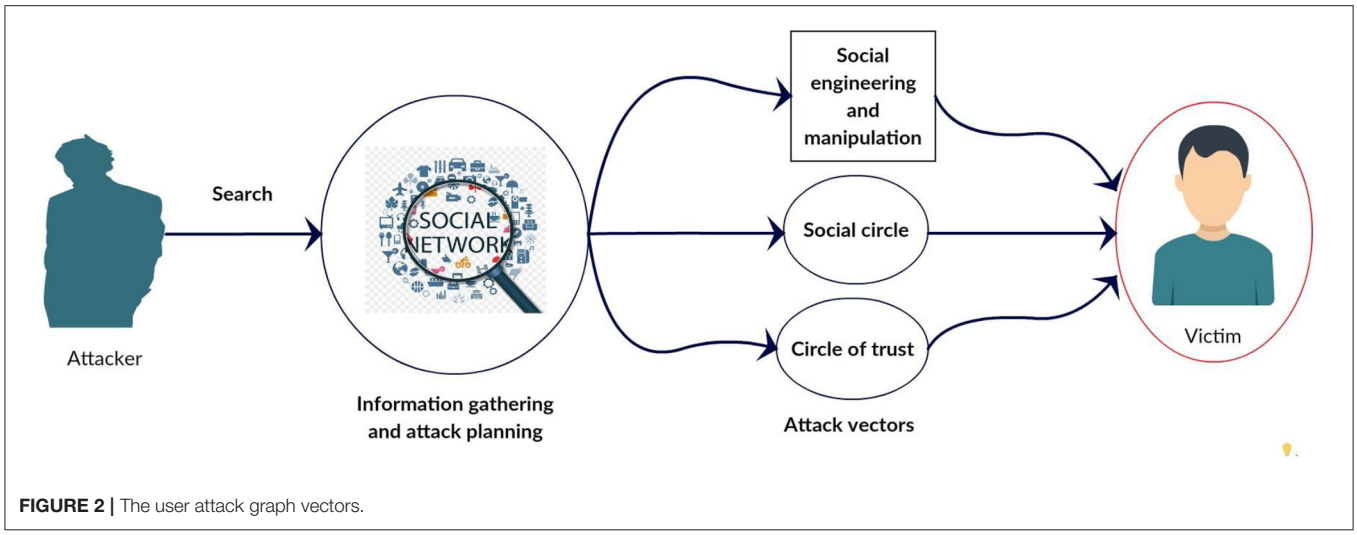

FIGURE 2 | The user attack graph vectors.

They puts themselves and all users with whom they interact in danger. The risk factor for any user increases logically with the increase of the vulnerable users with whom they interact. This factor also increases if the user has a hacker in their entourage, which gives the latter a better angle of attack.

Any user is said to be compromised **CM** when they have malware on their device, which gives the hacker full control over the device and a better opportunity to spread the malware to the user's entourage.

Any user is said to be potentially compromised **PC** if they have a compromised user in the circle of trust with whom they frequently interact, so the malware will be exchanged among files or emails.

From the above, the following vulnerability metrics were established.

1. User x is vulnerable if there is a vulnerable user y in his social circle.

$$\boldsymbol{V(x)} = \{1 if (x \in \boldsymbol{SCi}) \wedge (\exists y \epsilon \, \boldsymbol{lSCi} \wedge \boldsymbol{V}(y) = 1), 0 \; else\}$$

2. User x is highly vulnerable if there are many vulnerable users in his social circle.

$$\boldsymbol{HV(x)} = \{1 if (x \in \boldsymbol{SCi}) \wedge (\exists (y1, y2.., yn) \in \boldsymbol{SCi} \wedge \boldsymbol{V}(y1, y2, .., yn) = 1), 0 \; else\}$$

3. User x is highly vulnerable if there is a vulnerable user y who belongs to his circle of trust.

$$\boldsymbol{HV(x)} = \{1 if (\exists y \in \boldsymbol{CTx} \wedge \boldsymbol{V(y)} = 1), 0 \; else\}$$

4. User x is highly vulnerable if there is a hacker z who belongs to his social circle.

$$\boldsymbol{HV(x)} = \{1 if (x \in \boldsymbol{SCi}) \wedge (\exists z \in \boldsymbol{SCi} \wedge \boldsymbol{HK(z)} = 1), 0 \; else\}$$

5. User x is highly vulnerable if there is a compromised User y in his social circle.

$$\boldsymbol{HV(x)} = \{1 if (x \in \boldsymbol{SCi}) \wedge (\exists y \in \boldsymbol{SCi} \wedge \boldsymbol{CM}(y) = 1), 0 \; else\}$$

6. User x is potentially compromised if there is a compromised user y in his circle of trust.

$$\boldsymbol{PC(x)} = \{1 if (\exists y \in \boldsymbol{CTx} \wedge \boldsymbol{CM(y)} = 1), 0 \; else\}$$

The reasons for cyber-attacks against critical systems tend to be consistent same (financial gain, fame, etc.). When the attack vector changes, it involves the use of different techniques and methods that exploit different kinds of weaknesses in human behavior, such as naivety and neglect. The attacker creates a false perception of the situation, which leads the users to unintentionally perform the action that attacker desires.

The model above (**Figure 3**) represents the different active classes in a user-oriented attack. User behavior plays a significant role in the success of these attacks, as their tendency to disclose personal and professional information builds the knowledge base that the hacker uses in attacks. Social networks are a goldmine for extracting this information. The hacker builds one or more attack plans depending on the information found. Attack formulation varies, depending on the chosen method and disclosed information. For example, if the victim's address is among the information revealed, the hacker can access the victim's personal wireless point to sniff-out passwords or place malware inside their personal network. Alternatively, if the email address is disclosed, the hacker is more likely to send spear phishing attacks.

This section has discussed the various attack vectors and techniques used against end-users. This scheme of cyber-attacks has caused devastating damage in recent years, emphasizing the need to find useful and practical defense solutions.

SECURITY TRAINING MODEL: STRIM

Maintaining information security and protecting data assets remains a principal concern for most organizations. Human factors are still regarded as the root cause of many data breaches (Symantec, 2018), damaging reputations and leading to financial

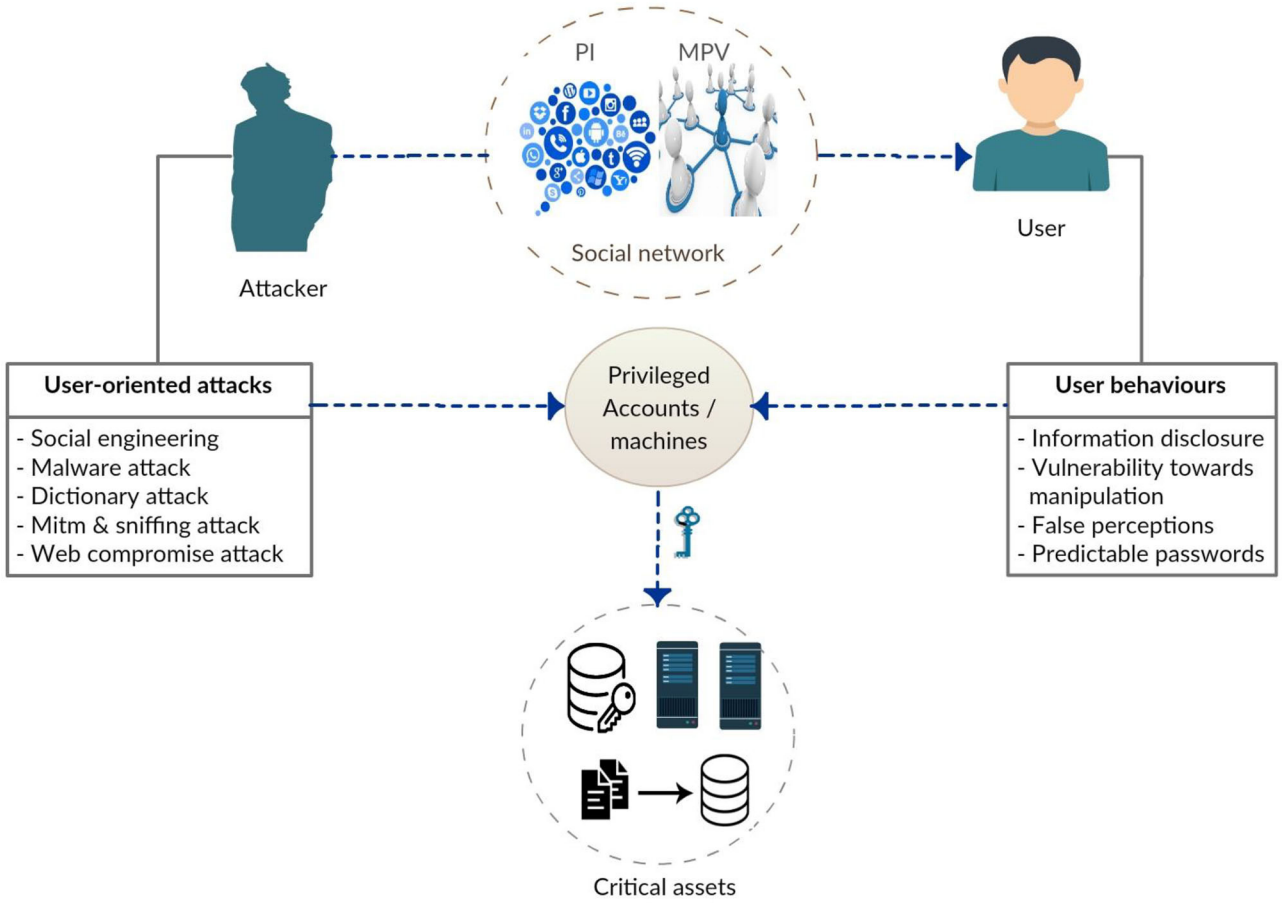

FIGURE 3 | The architecture of a user-oriented attack. PI, Privacy Invasion, MPV, Multi-Party Vulnerability.

loss. Organizations can no longer depend solely on technology and technical solutions to address security problems.

Many security reports use the phrase "sophisticated cyber-attack" to describe data breach cases and companies are on the defensive as soon as a breach is announced. This term is commonly used to avoid responsibility and embarrassment in explaining to clients how private and sensitive data was not appropriately safeguarded. The word sophisticated indicates that it was an attack that was cleverly studied and prepared over several stages. This includes work done before and after a breach, how an attacker penetrates and maneuvers silently within a network and steals sensitive data without leaving a trace. Most so-called sophisticated attacks start with methods that are more simple than extraordinary and are planned using information that is already in the public domain—typically beginning with spear-phishing or exploits that vendors have been already released a patch for Uchill (2019).

The success of any security awareness program is related to the success of all users without exception because a single weak user can lead to a complete security failure (Solove, 2019). Hence, user-based threats need a user-centric solution that focuses on the individual vulnerabilities of each user and their causes. This section details a theoretical user-based security awareness and training model. This model is personalized according to the user's abilities and their security knowledge level. It enables users to recognize security threats and personalized cyber-attacks, and to respond accordingly.

Security Awareness Solutions

The implementation of ongoing security training activities is one approach in improving safety behavior and security culture. Safety awareness is an essential factor in mitigating the risk of data breaches in organizations (Sood and Enbody, 2013) and users must understand and be prepared to assume their role in the security process in an effective way. According to Gartner (2019), 60% of large/enterprise organizations will have comprehensive security awareness training programs by 2022. The urgent need for awareness training has led to the creation of security awareness and training programs, such as Symantec.com, Sans.org, Kaspersky.com, Eset.com, and Proofpoint.com, and other solutions that use education and simulation to reinforce technical cybersecurity hygiene skills among employees.

In their latest Magic Quadrant report for Security Awareness Computer-Based Training, Gartner (2019) have made a comparative analysis of the different well-known end-user security awareness solutions. The study was based on various criteria, such as gamification, multi-language support, and pricing. These security awareness programs are very good at introducing different cybersecurity concepts in a smooth and straightforward way. They explain to users the various security issues using a high-quality creative video, which is proven to be one of many effective learning methods (Woolfitt, 2015). Creative videos are used to capture the users' attention and help them remember the concepts introduced to them.

In addition, awareness programs provide users with adapted multi-level courses that are compatible with their different knowledge levels in the field of information security. These programs also provide systems administrators with automated tools to manage the awareness process and to create automated tests for users. However, successful cyber-attacks against large companies, even those with awareness training programs like Yahoo and RSA, have proven that this is still not enough to guarantee the security of users and organizations against constantly emerging and highly sophisticated personalized attacks. This is due to various reasons:

1. The theoretical understanding of what a cyber-attack is does not guarantee that a user will be able to react when he faces a real attack scenario.
2. The simulations of cyber-attacks during a learning process are easy to detect, while real user-oriented attacks are very personalized and unpredictable.
3. Automated spear-phishing tests are made by a system administrator who lacks the skills of a real hacker to create an unpredictable and highly sophisticated attack.
4. The automated vulnerability tests are designed for a large number of users, whereas in a real attack, a hacker takes their time, collecting every possible piece of personal information about the victim in planning the attack.

Given the above factors, security awareness training programs need to be adapted and improved continuously to train and help users to deal with the emerging cyber threats and sophisticated cyber-attacks. It is not enough to explain what a cyber-attack is: users need to understand the magnitude of the threat, how it is prepared, and what makes them vulnerable. Finally, it is crucial to test their reactions in the context of a real-world threat. This ensures that they will react appropriately when facing a cyber-attack and that they are able to protect themselves, their organizations, and to transmit good security practices to those around them.

STRIM Objectives

Effective security is not about a single good solution but multiple layered solutions. The success of the security process is about encouraging users to update their security perspective and improve their knowledge, by motivating them to learn how to react better.

STRIM, as shown in **Figure 4**, is a design model for a user-based security training platform that will be developed in our future work. It is proposed as an improvement that adapts security awareness and training programs, responding to the needs of modern cybersecurity.

STRIM aims to:

1. Identify the human threat.
2. Measure the user's vulnerability.
3. Develop critical thinking among users.
4. Improve user's detection rate of cyber-threats.
5. Establish security behavior.

In awareness activities, the user is the recipient of information, whereas the user in a training test has a more active role. The main objective of STRIM is to satisfy the following main questions.

Q1. Do users know they are a prime target of cyber-attacks?
Q2. Do they know what makes them vulnerable to these attacks?
Q3. Do they know how these attacks are carried out?
Q4. Do they know that they should do something?
Q5. Do they know what they are supposed to do?
Q6. Are they motivated enough to do it?
Q7. Are they capable of doing it?
Q8. Would they successfully do it?

The User's Characteristics

Personal characteristics play an essential role in defining a user's vulnerability, their perceptions of cybersecurity and awareness of content which affects engagement with programs or security policies. These characteristics include security knowledge, attitudes, behavior, and experience. Personal characteristics vary from one user to another; therefore, every user will be categorized, so that they can start with the appropriate content related to their security-knowledge level. Moreover, each user will be tempted by the vector to which they are most vulnerable.

Cognitive Ability

Cognitive ability is defined as the user's ability to memorize or to comprehend the knowledge introduced to them. It groups five elements, planning, inhibition, flexibility, judgment, and auto-criticizing. This ability is affected by the teaching methods and the extent of user motivation and engagement. A different set of techniques can be used to ensure the efficiency of the awareness process, such as user implication, stories of real cyber incidents, and the interactivity between users.

Cognitive Bias

As mentioned in section Overview of the User-Oriented Attacks, a user's reasoning can be affected by different cognitive biases. Most users do not place enough importance on security, because they often rely on one basic idea (why me?). Most users consider they have an uninteresting profile, which leads to a failure to consider that they can be attacked and used as a bridge to reach further targets, like their organizations or social circle. Most users tend to use these biases in situations where they feel stress, fear, pressure, and anxiousness.

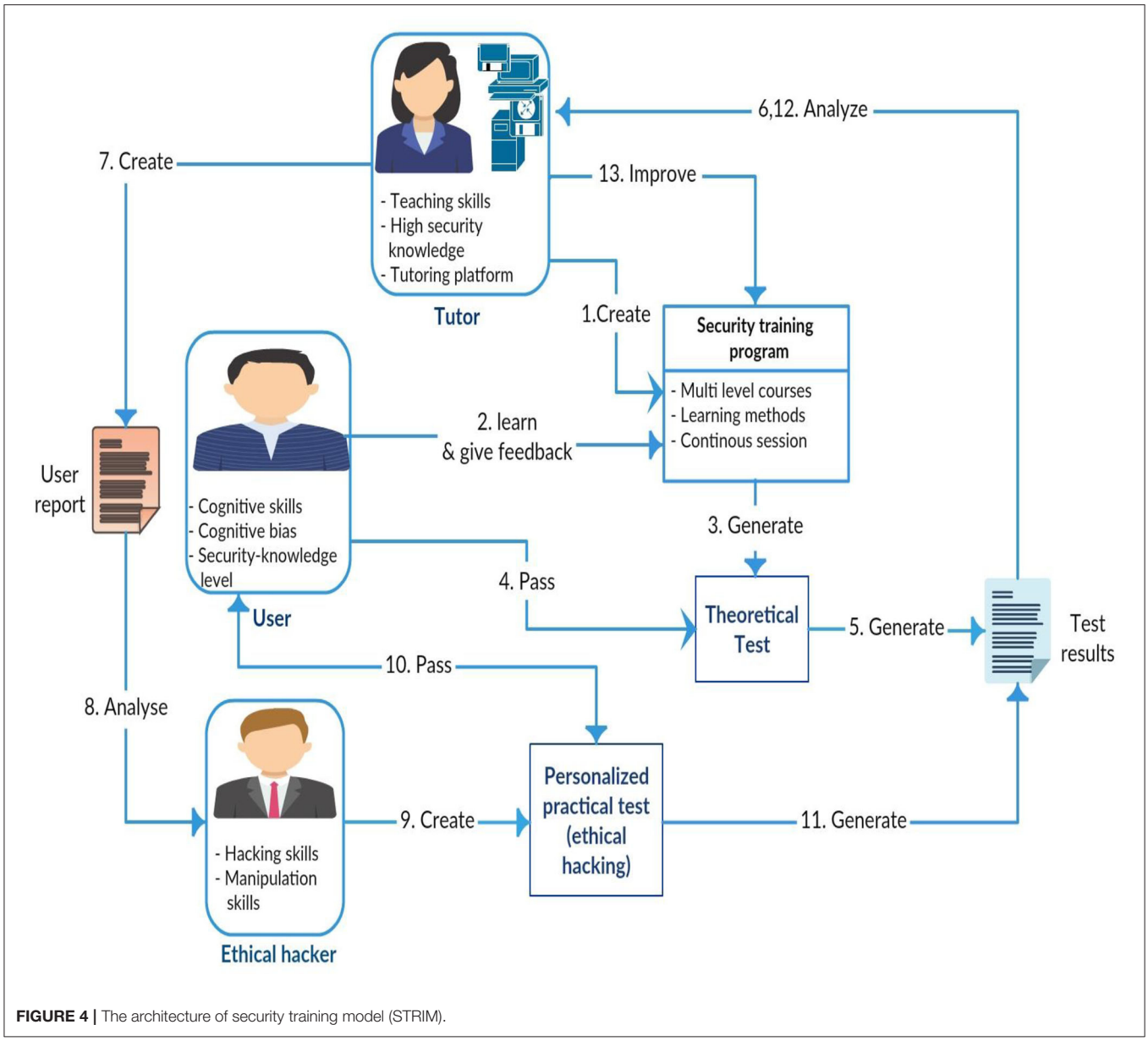

FIGURE 4 | The architecture of security training model (STRIM).

User's Background

This includes the personal variables that impact the user, including demographics and experience, knowledge, culture, education, attitudes, motivations, age, beliefs, incentives, etc. It is essential to consider who these users are likely to be and what their characteristics suggest about their behavior. It is also important to consider their relevant knowledge and previous experience. These personal variables can influence the ability of a user to understand and their capacity for action.

The above-mentioned criteria play a critical role in defining the vulnerability of users. While two users seem similar, they can also be different to others. This fact should always be taken into consideration when we consider two different users who are employed in organization X in country Y. The first user A is native to the country and openly shares their private life and thoughts on Facebook social networks and, like a lot of people, share concerns and worries about the situation of the Covid-19 pandemic. The second user, B is an immigrant in country Y and is more hesitant in sharing their private life on social networks because of their background. However, their LinkedIn profile indicates that they moved country and have worked in organization X since their arrival in country Y a year ago.

Classical approaches would test both employees A and B using the same procedure, for example, a spear-phishing which impersonates their superiors demanding an urgent task be done, with a malicious attachment. This kind of phishing can be easily detected by both users. However, this approach gives no guarantee that the two users will succeed every

time, as both users succeeded because the test was somewhat standard and predictable. This might vary if we test these two users in a personal context that takes into consideration their different backgrounds, using disclosed information about each one of them. For example, user A would be tested with spear-phishing containing malicious links supposedly sent by the health ministry, with information regarding the epidemic, good practices to be followed, and measures that will be applied. User B would then be tested using a spear-phishing with a malicious attachment from the immigration department, with information on immigration law and steps to be followed, such as completing a form.

A successful user-oriented attack exploits a situation that preoccupies the user and should be considered in security awareness and training process.

STRIM Architecture

As described in the section that follows, STRIM is a continuous process that consists of elements and interactions.

STRIM is structured as follows:

1. The tutor creates security awareness courses; each course is divided into three difficulty levels to be adapted to the different levels of users' knowledge in computer security. The user begins a security course and gets the scientific materials corresponding to their knowledge level.
2. At the end of each session, a theoretical test is generated to evaluate the users.
3. The user is invited to pass a test each to validate the acquired knowledge.
4. After the user validates their test, a test result is generated with a knowledge score and sent to the tutor.
5. The tutor analyzes the user's results and progress during the different sessions.
6. The tutor creates and sends a user vulnerability report to the ethical hacker.
7. The ethical hacker analyzes the user's report and profile; then tracks the available online information to plan an ethical cyber-attack against the user.
8. The ethical hacker creates a surprising personalized ethical hacking test to evaluate the user.
9. The user is put under a real hacking scenario to test their abilities.
10. The ethical hacker analyzes the user's performance in dealing with the attack and creates a report with privacy and awareness scores.
11. The tutor analyzes each user's results separately to analyze their progress and issues.
12. The tutor adapts and improves the security content to address the users' vulnerabilities.

The Actors

This model has three main actors, the user who represents the learner, the tutor who represent the teacher, and the ethical hacker who creates the final practical test.

The user is the learner who receives the security courses and whose actions will impact the organization's security. Each user has a different set of characteristics (knowledge, experience, behavior, etc.) that affects his learning progress and cybersecurity skills.

The tutor is the teacher who creates and improves the content of security courses in concordance with users' learning preferences and their results continuously. A tutor must have teaching skills, high-security knowledge, and experience in using tutoring platforms and creating courses.

The ethical hacker also called "White Hat," who is a professional hacker with high technical and social engineering skills. They create personalized tests to search for and exploit the vulnerabilities of the target users. In this context, they use the same tools and knowledge as any malicious hacker, but legitimately and lawfully.

The Security Awareness Courses

The awareness courses define the information processing step, which includes comprehension and knowledge acquisition; multi-level courses are used to categorize each user depending on their previous experience and knowledge in security. To satisfy the different learning preferences, our model consists of two information processing methods, which are interactive sessions and e-learning courses. The efficiency and the difficulty of every session are defined by the users' evaluation and their theoretical test results.

The courses are divided into three levels to help each user to adjust their security knowledge level.

The first level is an introduction to security. It contains a detailed explication on the basic elements of cybersecurity, like malware, spam, anti-viruses, network architecture and communication protocols to teach users to introduce the user to the essential elements of cybersecurity.

The second level provides further understanding of personalized cyber-attacks and sensitive personal information. Users are shown the relation between the attack vectors and their disclosed information besides its impact on the attack formulation. Moreover, users are provided with methods on the correct use of privacy settings besides the many information harvesting techniques. Users are also shown different psychological and manipulation techniques and cognitive bias that makes them vulnerable to social engineering scenarios.

The third level provides an advanced technical analysis of cyber-attacks and protective measures. Users are shown various techniques, such as examining email headers to detect spear phishing, inspect HTML code, and compare IP addresses, and avoid malicious links. Moreover, users are taught how to use adjusted network configuration, security tools, two factor authentication, and to secure network connections to prevent and detect attacks (Sandbox tests, VPN, etc.).

The Training Tests

This comprehensive training program is set to validate users' awareness and continuously test whether they can handle cyber threats. Even when users comprehend a security course, understand how to apply it, and identify the situation where they should apply it, failures may still occur, for instance if they are not

capable of taking appropriate actions. This model uses two forms of tests to measure users' progress and vulnerability scores.

The theoretical test is a short test, often in the form of a quiz. The tutor creates this test after each session to validate whether users have understood the security content or not, and to what extent are they able to identify the cyber threats that are related to the lessons.

The personalized test is a sort of a practical exam created by an ethical hacker. The user is set in the context of a real cyber-attack (spear phishing, pretexting, drive-by download, etc.) to test whether they will successfully identify the threat or not. A personalized practical test is created according to the report created by the tutor. This attack is personalized depending on the character of the user, their background, and the disclosed information that the user in question has online (e.g., the ethical hacker can impersonate one of the user's friends on a social network and send them a malicious link).

User feedback is a set of questions about the content presented at each session, gathering users' impressions of the content's clarity and difficulty, and opinion on the related security measures. It is presented clearly and with the appropriate amount of information. Taking the user's feedback into account also helps to understand how motivated users in their willingness to commit to the security process.

User results define the progress and the improvement of users during the sessions. This result is calculated from the following different scores obtained during the theoretical and practical tests.

Security knowledge score (Sks) is defined by the user's results in the theoretical test on the various aspects and techniques of cyber-attacks and cybersecurity in general.

Privacy score (Ps) is given by the ethical hacker through the practical test, depending on the user's disclosed information on social networks, their sensitivity, and their accessibility.

Awareness score (As) is measured by the user's success or failure in the practical personalized test, which defines whether they can detect and avoid cyber-threats or not.

The Interactions

STRIM is based on the subsequent interactions between the three actors.

User-tutor: The tutor or teacher in this context transmits their knowledge to the user either directly in the interactive courses, or indirectly through the e-learning content. They then analyze the user's results in both tests to create a detailed report.

Tutor-ethical hacker: Creates an adapted personalized test using a user report from the tutor, and then sends the test results back to the tutor.

Ethical hacker-user: An ethical personalized hacking scenario is set by the hacker to test the user's security skills in the context of a sudden real cyber-attack, like a spear-phishing email.

Tutor-security courses: The security content is created and continuously improved by the tutor, to ensure its quality and efficiency with respect to users' needs, and new emerging cyber threats.

User-security courses: The user takes the security course level that suits them the best, according to their pre-knowledge. They also choose the teaching method that satisfies their learning preference, either interactive courses or through e-learning courses. As with any training models, a strategy is needed to achieve the planned goals.

The Security Training Strategy

There are numerous strategies to improve security. The first and by far the most used, is user awareness and education. Therefore, it is essential to improve the security behavior of every single user because the success of any security process is related to the success of all its elements. This model aims for a user transformation, from being the weakest link to a much more active role that can detect attacks, report them, and transmit good security practices to their own entourage. Our proposed model focuses on the following elements.

Teaching Privacy

The best way to teach privacy is to show how risky the situation is without it, and privacy underpins this need to address and protect users (Solove, 2019). The users are shown the many techniques of tracking their disclosed information (Pipl[2], People finder[3], White pages[4]), pictures and activities (Google image reverse[5]), and the different ways in which this disclosed information on social networks can be turned into precious elements that construct the full picture, enabling the planning a sophisticated cyber-attack. As a convenient solution, users are taught how to use appropriate privacy parameters on different social network platforms to prevent information disclosure. That way, users are able to link their unconscious actions to the possible risks to their organization.

Cyber-Attack Techniques

Users are shown the various techniques through which they can be hacked, including spear phishing, pretexting, fake landing pages, and malicious attachments, etc. with information on related, devastating real-world breaches, in order to motivate the user, get their attention, and help them stay aware. The course also focuses on techniques and precautions in detecting and escaping cyber-attacks (checking mail headers, sandbox executions, etc.).

Critical Thinking

Critical thinking is an objective, logical, and consistent analysis that enables people to reach a rational judgment (Stanovich, 2009). It is a key attribute in improving safe behavior. By focusing on developing a sense of skepticism and rationality among users, they are trained to refuse to do or to admit things without critical examination. They are taught to think about the logical causes and the possible consequences of the different decisions they make, whether online or off. Moreover, their vulnerability metrics are studied in detail to help each user when calculating risks

[2]Pipl. Available online at: https://pipl.com/ (accessed September 6, 2019).

[3]People Finders. Available online at: https://www.peoplefinders.com/ (accessed August 5, 2019).

[4]White pages. Available online at: https://www.whitepages.com/ (accessed December 7, 2019).

[5]Google Images. Available online at: https://images.google.com/ (accessed October 5, 2019).

in each online interaction. It aims not only to help users by adopting a vigilant and attentive behavior, but also to transmit safe practices to those around them.

On a practical level, users must think twice before giving information or opening any link. In this context, users are shown many different examples showing how content that seems reasonable and clean (like fake pages) can hide malicious elements or how a seemingly legitimate mail from a trusted source (spoofed email) is just a sophisticated form of phishing that is difficult to detected.

Security and Privacy Critical Thinking Model

Information is a key element in building user-oriented attacks. Attackers are more likely to target the users on whom they have the most information. Risk of cyber-attack is closely linked to personal information disclosure, especially if that information is not safeguarded.

As shown below in **Figure 5**, the security and privacy critical thinking model depicts the flow of action in online security and privacy and how information should be perceived and handled by an online user. It explains the logical steps and questions that users need to think about when they are managing their personal information online, to push them into thinking about risks. The model is designed to help users measure their online actions using rational thinking instead of cognitive bias, a guideline to aid users in decision making and in its improvement.

The first step in protecting users against personalized attacks is to reduce the risk of being attacked. The model begins by questioning the quantity, the emplacement, and the sensitivity of the information that users have online.

In the case of public information, users are encouraged to classify attacks that may be generated using that information and to think about whether they will be able to handle it or not. Otherwise, in the case of private information (on social networks, for example), users must apply the vulnerability metrics to their online entourage, calculate the risks, think, and decide whether the data in question should be deleted or kept under appropriate privacy measures.

This model only covers part of the problems related to information disclosure. Users are not the only person responsible for privacy issues and containing sensitive personal information are compromised daily in data breaches. These data vary between names, dates of birth, addresses, banking information, social insurance numbers, and credentials. Whether they are aware of

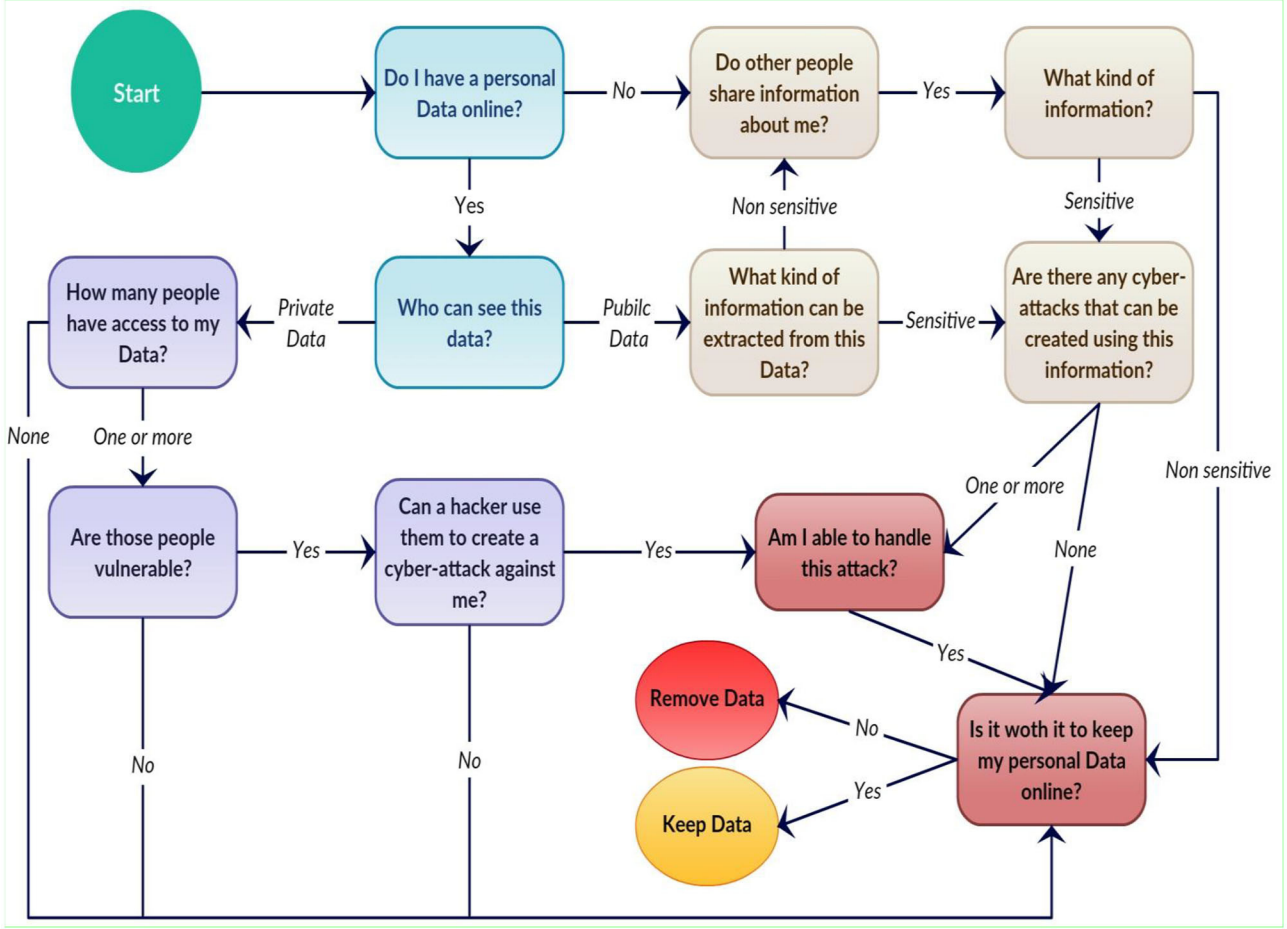

FIGURE 5 | Security and privacy critical thinking model.

it or not, most users have been affected to varying degrees by breaches. Indeed, users need to think about the dangers of re-using passwords, giving personal information when they don't have to, or using professional and personal emails to access websites online.

Useful Technical Solutions

There are a variety of technical solutions that can help and to some extent protect sensitive data, including:

Strong passwords: The creation of a strong password is important in protecting a user's online identity, a good password is difficult to guess or to decode, which must be quite long, complicated (a mixture of uppercase and lowercase letters, numbers, and special characters), and finally which must not be kept on a connected device.

Multi-factor authentication: Is an authentication method in which a user device is granted access only after successfully presenting one or more pieces of evidence besides credentials (For example, a code sent over SMS).

Encrypted connection (VPN): A virtual private network is a service that provides secure connection through an encrypted tunnel to preserve online privacy. VPN encrypts data when it is sent over a public network, which makes the data unreadable, protecting it from sniffing and man in the middle attacks.

Checking the website's SSL certificate: SSL is generally used to ensure data and connects safety and securely between the web server and the browser. If available, this certificate shows a padlock beside the "https" protocol in the link tab of the browser.

***Checking email header*:** Email header verification allows users to identify suspicious items in the received mails. In SMTP, the P1 MAIL FROM header is used to authenticate the sender of an email with a specific domain name. The P2 FROM header is used to display a sender alias; this field can be manipulated to show the email as if it were sent from a different source (Kirschner, 2019). Users must check the conformity between those two headers to detect spoofed emails.

Hovering over links: Phishing and fraudulent websites use deceptive methods to fool users into giving their credentials and sensitive information. What is shown on the link description is often different from where that link leads. Therefore, the user must hover the mouse over any link to see the full description and check its validity before clicking it.

All the previously mentioned elements represent the core learning outcomes of this proposed package. Therefore, it is essential to ensure that these elements are presented in a coherent and smooth manner and under a logical structure, to ensure its usability.

The Usability of the Model

Usability is the measure of the interactive user experience associated with a learning system. This research took into consideration the different user characteristics shown in **Table 1**. To satisfy the possible requirements, security should be perceived as a challenging concept rather than a set of boring instructions to be followed. This set of personal characteristics (motivation, experience, and knowledge) and system characteristics (conformity, attractivity) affects the degree of the user's engagement and their participation in the success of the security process.

TABLE 1 | User's characteristics and potential requirements.

Characteristics	Potential user requirements
Previous security training	- Ensure the system's conformity with different level of security knowledge
Knowledge of the task	- Highly supportive interfaces - Logical structure - Clear terms and examples
Previous experience with e-learning	- Create attractive interfaces - Use supportive dialogues
Motivation to use	- A challenging concept - Involving the users - Measured progress
Frequency of use	- Commitment - Planned goals - Weekly sessions
Discretion to use	- Attractive concept - Ensure that results can be achieved quickly

Satisfaction of the previously mentioned criteria is very important in ensuring the system's ease of use for the different users, which in turn improves its efficiency.

STRIM is supposed to be implemented on an online e-learning platform to give users the possibility to use it at the time and place they want. The use of quizzes and different scores introduce a playful and challenging concept for users who are supposed to improve their scores over time. This progress allows them to consider the training process as self-improvement and as a personal gain rather than additional training that they must pass for their company. On the tutor's side, result scores can be used to identify the human threat among employees and measure their vulnerability, following their progress over time.

The global efficiency of the system will be calculated by the tutor once all users have passed the practical personalized test. If the number of users or employees who will pass the test successfully increases over time, then the program is successful. The tutor must review and modify the content again, depending on the results.

The Ethical Aspect

Like any other form of attack, cyber-attacks are physical, and it is therefore important to educate employees using a real-life test in order to create a vigilant system user. These users need to gain experience in dealing with cybercrime and protecting confidential data. The ethical cyber-attack is now a necessary method of creating an awareness solution, especially for users based at companies that hold sensitive information about their customers, like banks, insurance companies, hospitals, etc.

Regarding the ethical side, there are inevitably many questions concerning this proposed training method. The most important is how can these ethical attacks respect the privacy of employees while using the same techniques as hackers?

Firstly, employee permissions are required before training. They will be informed about all the training steps, including the practical test, the purpose, and motivation. The users must understand why these tests are necessary for their safety, that of the organization, and that of their clients.

Secondly, the practical test is the last step in the training process. The users will be prepared in advance, and nobody will be tested using an ethical cyber-attack before they have passed the theoretical tests where they are provided with information about cyber-attacks, the methods used by hackers, and the protection of private data. Moreover, no malicious malware will be used in the test process, but merely an encrypted backdoor with limited functions to indicate to the ethical hacker if the user has failed the test. Afterward, the evaluation is made based on the test result and the amount of sensitive information that the ethical hacker finds online about the user in question.

Finally, the scale of cyber-attacks and the fact that they are now used more often obliges us to be prepared in an adequate way to defend ourselves. We live in a hyper-connected world where we must enter our confidential data everywhere to benefit from the services that we need. All users have the right to be sure that the people who have access to their data are well able to protect them. We strongly believe that an employee needs to be able to react correctly to a cyber-attack, keep their private data safe on social networks, and be able to keep sensitive data secure.

This proposed security awareness and training model aims to improve security awareness and validate the learning process, using real ethical attacks as a test, which act as an effective way to enhance user awareness and teach security. This model is an important aspect of efficient cyber security policy and establishing security-conscious behaviors among users/employees.

CONCLUSIONS

To date, there is little academic research dedicated to sophisticated cyber-attacks that target users. This paper has provided a description of common attack methods and scenarios in modern user-oriented attacks. It studied the relationship between type, quantity, and sensitivity of disclosed personal information, the attack vectors that an offender can adopt in response to this information, and theories of psychological manipulation and cognitive bias that may affect a user's behavior. This research has also explored the impact of the group on one's vulnerability in a social network. A detailed understanding of these factors is essential in developing appropriate countermeasures and in protecting online users against sophisticated attacks. To address this our research involved a comprehensive study of user-oriented attack technics and vectors. Using real-world examples, it also explained the different stages of attack formulation, starting with the information gathering process, the attack plan, the choice of the attack vector, the deceptive manipulation approach, and the technical methods of cyber-attack.

This study also furthers understanding of personalized user-oriented cyber-attacks. On the one hand, it highlights the impact of low privacy and personal information disclosure as a knowledge-base for these attacks, explaining the various forms of psychological manipulation used in different attack scenarios, and identifying the cognitive bias that leads to human failure in assessing cyber-attacks. On the other hand, and to the best of our knowledge, this is the first study to introduce and explain how the *social circle* and the *circle of trust* could be used as attack vectors, with detailed explanation of possible approaches and attack methodologies, which have not been addressed in previous research. To conclude, the paper proposed *metrics* as a way of quantifying and measuring the user's vulnerability. This is calculated as a risk factor that varies depending on the user's interactions and the vulnerability of their digital entourage.

The second part of our research has proposed a *theoretical user-based security training model, STRIM*. It is a model that aims to satisfy cybersecurity requirements, by creating user-awareness of content that focuses on various new and emerging threats. STRIM incorporates non-technical aspects such as manipulation, cognitive bias, and security behavior. Every user is trained to detect and avoid different kinds of cyber-attacks and their progress and vulnerabilities are tested by an ethical hacker, who tests user responses to a cyber-attack. The tutor is then able to adapt and improve security content depending on users' scores, progress, and results. Our model extends the state of this area, by including a novel approach and strategies of effective learning, training, and awareness as a key part of the process of developing security. This model provides a solution that aims to help organizations improve security behavior among their employees.

This research paper first studied security awareness solutions, to explain why these solutions may not satisfy today's security requirements. It then presented in detail the different elements that constitute the architecture of STRIM. After that, it examined the approaches used to train users and teach them about the current cyber-attacks and explained the impact of their disclosed information in creating vulnerabilities.

This paper also discussed the personal characteristics that should be taken into account during the training process and explained the importance of privacy and its impact on user's safety. To conclude, the second part of this research provides a model for critical thinking in security and privacy, a series of actions and questions that act as a guideline when managing personal data online. This model focuses on developing a sense of skepticism and rationality among users by inviting them to refuse or accept digital interactions without thinking about the consequences. However, this proposed solution cannot solve all the security threats at once. For example, Zero-day exploits and social engineering scenarios are unpredictable and it is very difficult to defend against them. STRIM is a partial effort to improve security awareness and reduce the security flaws caused by human factors, and aims to give users the means to play a more active role in the overall process of security.

Our solution ensures that employees are aware and up to date and can understand, detect, and report cyber-threats. The commitment of all users is necessary for success. However, the ethical hacking aspect may be considered by some users as an invasion of their privacy, which poses a further obstacle to training and creates a difficult task for systems administrators,

who will need to convince users about the urgent need for these tests. Despite all this, humanity is stuck in a cyberwar with limited choices. Either organizations prepare employees, enabling them to deal efficiently danger on the internet, or they need to go back dozens of years to a time when every sensitive asset was indispensable and required continuous monitoring by humans.

One can conclude that a user's vulnerability is defined depending on the user's security knowledge, their online privacy, and the vulnerability of their digital entourage. The type of personal device and the context in which the user uses it during the interaction, are also considered as factors that may influence their vulnerability. Future work will focus on the development of a security training platform based on the STRIM design model's characteristics and functionalities. This will allow us to compare the performance of this platform with other security awareness platforms. Moreover, it will enable an examination of the effect of the device on users (e.g., personal computer, tablet, or smartphone) and information processing. For example, are users more likely to open a spear phishing mail when they are using their smartphone outside due to the distraction and the anticipated brevity of the interaction (e.g., driving or shopping)? They may tend to evade malicious links on smartphones because they are less likely to open links and websites due to these distractions and the small size of the screen. However, users are at greater risk of installing malware on smartphones or tablets because most of them only use anti-viruses on computers.

When it comes to cyber-attacks, knowledge is the real power. An aware user who knows how to detect and report a an attack is better than one who does not. Cyber threats do not exclusively target enterprises, they also threaten the privacy of the individuals. Attacks targeting people and their data are increasing and are more frequent and knowing how to protect oneself is an absolute necessity. Security training is a big step forward in facing these threats. The internet plays a critical role in our lives, whether in education, economics, art, or any other aspects of life. Knowing how to use the internet is as important as mental computation, driving, or any obvious skill in people's lives. Given the ubiquity of the internet in our everyday lives, basics such as privacy, ethics, safe behavior, and online protection should form part of early education and even start in early childhood.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding authors.

AUTHOR CONTRIBUTIONS

AH redaction and implementation of attack models and architectures. EA correct, edit, and improve the paper content. All authors worked alongside to exchange ideas, create, and improve this paper.

REFERENCES

Adams, K. (2019). *Detecting and Preventing Man-in-the-Middle Attacks on an Encrypted Connection*. U.S. Patent No. 10/171,250. Alexandria, VA: Juniper Networks Inc.

Ahluwalia, R. (2000). An examination of psychological processes underlying resistance to persuasion. *J. Consumer Res.* 27, 217–232. doi: 10.1086/314321

Aïmeur, E., Brassard, G., and Molins, P. (2012). "Reconstructing profiles from information disseminated on the internet," in *2012 International Conference on Privacy, Security, Risk, and Trust and 2012 International Conference on Social Computing* (Amsterdam: IEEE), 875–883.

Aïmeur, E., Brassard, G., and Rioux, J. (2013). Data privacy: an end-user perspective. *Int. J. Comput. Netw. Commun. Secur.* 1, 237–250.

Akbar, N. (2014). *Analyzing persuasion principles in phishing emails* (Master's thesis). Enschede: University of Twente.

Bada, M., Sasse, A. M., and Nurse, J. R. (2019). Cyber security awareness campaigns: why do they fail to change behaviour? *arXiv.[Preprint].arXiv:1901.02672*.

Bain, K. (2004). *What the Best College Teachers Do*. Cambridge: Harvard University Press.

Baron, J. (2008). *Thinking and Deciding*. New York, NY: Cambridge University Press.

Berinato, S., and Bochman, A. (2019). Putting systems offline. *Harvard Bus. Rev.* 50–54.

Bezuidenhout, M., Mouton, F., and Venter, H. S. (2010). "Social engineering attack detection model: Seadm," in *2010 Information Security for South Africa* (Johannesburg: IEEE), 1–8.

Bulakh, V., and Gupta, M. (2015). "Characterizing credit card black markets on the web," in *Proceedings of the 24th International Conference on World Wide Web* (Florence: ACM), 1435–1440.

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., and Hartel, P. (2018). On the anatomy of social engineering attacks—a literature-based dissection of successful attacks. *J. Investig. Psychol. Offender Profil.* 15, 20–45. doi: 10.1002/jip.1482

Can, L., and Kaya, N. (2016). Social networking sites addiction and the effect of attitude towards social network advertising. *Procedia Soc. Behav. Sci.* 235, 484–492. doi: 10.1016/j.sbspro.2016.11.059

Chabrow, E. (2011). *Tricked RSA Worker Opened Backdoor to APT Attack*. Available online at: https://www.bankinfosecurity.com/tricked-rsa-worker-opened-backdoor-to-apt-attack-a-3504 (accessed October 10, 2019).

Cialdini, R. (2001). *Influence: The Six Principles of Persuasion*. NewYork, NY: HarperCollins e-Books. ISBN 978-0-06-18 9990-4.

Del Pozo, I., Iturralde, M., and Restrepo, F. (2018). "Social engineering: alication of psychology to information security," in *2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)* (Barcelona), 108–114.

Dinev, T., and Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *J. Assoc. Information Syst.* 8:23. doi: 10.17705/1jais.00133

Duman, S., Kalkan-Cakmakci, K., Egele, M., Robertson, W., and Kirda, E. (2016). "Emailprofiler: spear-phishing filtering with header and stylometric features of emails," in *2016 IEEE 40th Annual Computer Software and Alications Conference (COMPSAC),* Vol. 1 (Atlanta: IEEE), 408–416.

Epley, N., and Gilovich, T. (2001). Putting adjustment back in the anchoring and adjustment heuristic: differential processing of self-generated and experimenter-provided anchors. *Psycho Logical Sci.* 12, 391–396. doi: 10.1111/1467-9280.00372

Ficher, M. (2013). Syrian hackers claim AP hack that tied stock market by $136 billion. *The Washington Post*. Avaialble online at: https://www.washingtonpost.com/%20news/%20worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism%20/?utm_term=.%2048fe2c70f46f (accessed October 3, 2019).

Fleishman, G. (2018). *Equifax Data Breach, One Year Later: Obvious Errors and No Real Changes.* Available online at: http://fortune.com/2018/09/07/equifax-data-breach-one-year-anniversary/ (accessed September 23, 2019).

Furman, S., Theofanos, M. F., Choong, Y. Y., and Stanton, B. (2011). Basing cybersecurity training on user perceptions. *IEEE Secur. Privacy* 10, 40–49. doi: 10.1109/MSP.2011.180

Furnell, S., and Rajendran, A. (2012). Understanding the influences on information security behaviour. *Comput. Fraud Secur.* 3, 12–15. doi: 10.1016/S1361-3723(12)70053-2

Gartner (2019). *Magic Quadrant for Security Awareness Computer-Based Training.* Avaialble online at: https://www.gartner.com/doc/reprints?id=1-1OAYVTNP&ct=190723&st=sb (accessed August 15, 2019).

German, T. P., and Defeyter, M. A. (2000). Immunity to functional fixedness in young children. *Psychonomic Bull. Rev.* 7, 707–712. doi: 10.3758/BF03213010

Ghafir, I., Saleem, J., and Hammoudeh, M. (2018). Security threats to critical infrastructure: the human factor. *J. Supercomput.* 74, 4986–5002. doi: 10.1007/s11227-018-2337-2

Greene, K. K., Steves, M. P., Theofanos, M. F., and Kostick, J. (2018). "User context: an explanatory variable in phishing susceptibility," *in Proc. 2018 Workshop Usable Security (USEC 18)* (San Diego).

Hadnagy, C., and Fincher, M. (2015). *Phishing Dark Waters*. Hoboken, NJ: Wiley.

Heartfield, R., and Loukas, G. (2016). A taxonomy of attacks and a survey of defense mechanisms for semantic social engineering attacks. *ACM Comput. Surv.* 48:37. doi: 10.1145/2835375

Hong, J. (2012). The state of phishing attacks. *ACM Commun.* 55, 74–81. doi: 10.1145/2063176.2063197

Isaca (2018). *Top Cybersecurity Risks and Areas of Focus*. Isaca 2018 Report. EY. Available online at: http://www.isaca.org/chapters1/puget-sound/education/Documents/2018%20Emerging%20Trends%20in%20Cybersecurity%20-%20EY%20ISACA%20Presentation%20-%2020MAR.pdf (accessed August 20, 2019).

Ki-Aries, D., and Faily, S. (2017). Persona-centred information security awareness. *Comput. Secur.* 70, 663–674. doi: 10.1016/j.cose.2017.08.001

Kirschner, J. (2019). *How to Tell if an Email Has Been Spoofed*. Available online at: https://www.techlicious.com/how-to/how-to-tell-if-email-has-been-spoofed/ (accessed May 10, 2019).

Kotenko, I., Stepashkin, M., and Doynikova, E. (2011). "Security analysis of information systems taking into account social engineering attacks," in *2011 19th International Euromicro Conference on Parallel, Distributed, and Network-Based Processing* (IEEE), 611–618.

Krebs, B. (2018). *Tech Firm Ubiquiti Suffers $46 Million Cyberheist*. Available online at: https://krebsonsecurity.com/2015/08/tech-firm-ubiquiti-suffers-46m-cyberheist/ (accessed July 20, 2019).

Krombholz, K., Hobel, H., Huber, M., and Weil, E. (2015). Advanced social engineering attacks. *J. Information Security Alicat.* 22, 113–122. doi: 10.1016/j.jisa.2014.09.005

Leibenstein, H. (1950). Bandwagon, snob, and Veblen effects in the theory of consumers' demand. *Q. J. Econ.* 64, 183–207. doi: 10.2307/1882692

Lemay, A., and Leblanc, S. (2018). "Cognitive biases in cyber decision-making," in *ICCWS 2018 13th International Conference on Cyber Warfare and Security* (Washington, DC: Academic Conferences and Publishing Limited), 395–401.

Leon, F. R., Lundgren, R., Huapaya, A., Sinai, I., and Jennings, V. (2007). Challenging the courtesy bias interpretation of favorable clients' perceptions of family planning delivery. *Evaluat. Rev.* 31, 2442. doi: 10.1177/0193841X06289044

Neely, L. (2017). *Threat Landscape Survey: Users on the Front Line*. Sans Institute. Available online at: https://www.sans.org/readingroom/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910 (accessed December 19, 2019).

Niemelä, J., Hyönen, M., and Kangas, S. (2016). *Malware Protection.* U.S. Patent No. 9,501,644.

Pfleeger, S. L., Sasse, M. A., and Furnham, A. (2014). From weakest link to security hero: Transforming staff security behavior. *J. Homeland Security Emerg. Manage.* 11, 489–510. doi: 10.1515/jhsem-2014-0035

Plous, S. (1993). *The Psychology of Judgment and Decision Making*. NewYork, NY: Mcgraw-Hill Book Company.

Proofpoint (2018). *The Human Factor 2018, People-Centered Threats Define the Landscape.* Available online at: https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-wp-human-factor-report-2018-180425.pdf (accessed August 25, 2019).

Proofpoint (2019). *Proofpoint State of the Fish Report.* Available online at: https://info.wombatsecurity.com/hubfs/Wombat_Proofpoint_2019%20State%20of%20the%20Phish%20Report_Final.pdf (accessed November 7, 2019).

Rathore, S., Sharma, P. K., Loia, V., Jeong, Y. S., and Park, J. H. (2017). Social network security: Issues, challenges, threats, and solutions. *Information Sci.* 421, 43–69. doi: 10.1016/j.ins.2017.08.063

Reznik, M. (2012). Identity theft on social networking sites: developing issues of internet impersonation. *Touro L. Rev.* 29, 455–483.

Rubell, P. (2018). *Disclosure of Corporate Information Through the Use of Social Media: Identifying the Risks and Adopting Best Practices*. Available online at: https://www.academia.edu/4842241/Disclosure_of_Corporate_Information_Through_the_Use_of_Social_Media_Identifying_the_Risks_and_Adopting_Best_Practices (accessed November 12, 2019).

Sasse, M. A., Ashenden, D., and Lawrence, D. (2007). Human vulnerabilities in security systems. *White Paper. Cybersecurity KTN Human Factors* (Portsmouth, NH).

Schneier, B. (2003). *Security Is a Weakest-Link Problem. Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. NewYork, NY: Springer.

Solove, D. (2019). *Teaching Privacy Awareness*. Available online at: https://teachprivacy.com/effective-security-training/ (accessed November 2, 2019).

Sood, A. K., and Enbody, R. J. (2013). Targeted cyber-attacks: a superset of advanced persistent threat. *IEEE Security Privacy* 11, 54–61. doi: 10.1016/B978-0-12-800604-7.00002-4

Stanovich, K. E. (2009). *What Intelligence Tests Miss: The Psychology of Rational Thought*. New Heaven, CT: Yale University Press.

Such, J. M., and Criado, N. (2018). Multi-party privacy in social media. *Commun. ACM.* 61, 74–81. doi: 10.1145/3208039

Symantec (2018). *Symantec Internet Threat Security Report, 23*. Available online at: http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid$=$elq_ (accessed October 16, 2019).

Uchill, J. (2019). *The Myth of the Sophisticated Hacker.* Available online at: https://www.axios.com/sophisticated-hacker-cybersecurity-labour-party-f2137c08-0dec-4413-94d8-8f6729b6ec96.html (accessed April 20, 2020).

Van Boven, L., Loewenstein, G., Dunning, D., and Nordgren, L. F. (2013). "Changing places: a dual judgment model of empathy gaps in emotional perspective taking," in *Advances in Experimental Social Psychology*, eds M. Zanna and J. Olson (Burlington: Academic Press), 117–171.

Vishwanath, A., Herath, T., Chen, R., Wang, J., and Rao, H. R. (2011). Why do people get phished? testing individual differences in phishing vulnerability within an integrated information processing model. *Decision Suort Syst.* 51, 576–586. doi: 10.1016/j.dss.2011.03.002

Woolfitt, Z. (2015). *The Effective Use of Video in Higher Education.* Lectoraat Teaching, Learning, and Technology Inholland University of Alied Sciences. Available online at: https://www.inholland.nl/media/10230/the-effective-use-of-video-in-higher-education-woolfitt-october-2015.pdf (accessed September 20, 2019).

Zhang, B., Zhang, H., Li, M., Zhao, Q., and Huang, J. (2017). Trust traversal: a trusted link detection scheme in a social network. *Comput. Netw.* 120, 105–125. doi: 10.1016/j.comnet.2017.04.016

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.