How Aware Are You: A Study of Effectiveness of Existing User Education Methods

Pranali Divekar
Rochester Institute of Technology
Rochester, NY, USA
pd1267@rit.edu

ABSTRACT

In today's fast paced world, internet has become the bread and butter of everyone's life. From school students to older adults, everyone 'minds their own business'. Internet and security are like two sides of the same coin. With easier ways to access what you want to browse online comes the concern of privacy. Most users aren't aware of what they should and what they shouldn't click. This paper aims to understand the typical user patterns followed by naive users when they browse the internet. The lack of basic cybersecurity knowledge among the users is making it easy for attackers to carry out semantic attacks in order to find loopholes within the system and infiltrate it. An online study of twenty participants of varying age groups was conducted where they were asked to perform certain tasks on the internet and were monitored via a video conferencing platform followed by a short questionnaire testing their basic knowledge about internet security. It was found that 80% of the users were unaware of the basics norms that are to be followed online and surprisingly these users did not belong to any corporate organization. Thus, highlighting a section of the population that has been unknowingly excluded by the researchers.

Author Keywords

Internet; Security; Privacy; Cybersecurity.

CCS Concepts

•**Security and privacy** → **Usability in security and privacy;** Please use the 2012 Classifiers and see this link to embed them in the text: https://dl.acm.org/ccs/ccs_flat.cfm

INTRODUCTION

We see headlines everyday about scams happening around the world. Even today, many users do not understand the meaning of semantic attacks. As rightly explained in [5] semantic attacks are certain social engineering attacks used by attackers to fool the victims into thinking they are doing something but actually end up giving sensitive information to the attacker. It is manipulation of the user's perception and interpretation in order to obtain valuable information such as passwords, financial details or if the attack is on a large scale it might even breach the governments classified data. These attacks can be of various types [4] such as Phishing [5], Baiting, Shoulder Surfing [10], Typo-squatting, WiFi Evil Twin etc. The attackers make the website so appealing that the users find it hard to resist. There have been many valuable contributions by researchers in classifying these attacks for a better understanding of them. As explained in [6], spreading awareness about the stages of an attack – Orchestration, Exploitation, Execution is important because it helps to understand how deep rooted, we are into an attack.

As more and more naive audiences have started using the web extensively, finding loopholes in the systems has become a piece of cake for the attacker. Efforts have been taken in the direction of mitigating these attacks. Researchers have come up with models such as Social Engineering Attack Detection Model (SEADM) [3] and Social Engineering framework for Social Media (SESM) [13] in order to make the users working in corporate organizations aware. Despite various trainings and learning programs spreading security awareness, the system still remains vulnerable. Why? Are the established methods not adequate? Who is responsible to maintain the security of the system? Research shows that mechanisms devised like firewalls to counter these social engineering attacks are already placed in the system by the designers. Then why is there no toll on the scams that occur worldwide? The blame inescapably lands on the user. Hence, the researchers came up with user education methods like Anti-phishing tools [11], Human firewalls [9] etc. The rate of online scams reduced, but not significantly.

To analyze these issues and answer the questions above, there arose a need to tap on the effectiveness of these methods discussed above as there has been no research/survey conducted till date. This paper is an attempt to bridge the gap between the expected results which are to be achieved from the existing mechanisms incorporated in the systems and the practical result. It covers a survey conducted on an audience of twenty in order to understand where the general users stand with respect to knowledge of security. The audience was chosen randomly on purpose without the barrier of gender or age group. On conducting a through online survey that focused on understanding the user's thought process while making certain security decisions, understanding the challenges faced by users with respect to usability of the system I was able to get valuable results.

The results not only showed that the current methods are not properly employed but also showed that they have failed to reach an entire section of the population. The paper explains this point in the sections that follow. Secondly, on analyzing the browsing patterns of the users, the vulnerabilities of the

security system as a whole (i.e., including the users) became evident. Thirdly, the paper aims to point out certain enhancements that can be incorporated in the existing system design by the designers in order to employ the concept of invisible security.

The paper presents an elaborate analysis of the results found followed by a quick bar graph indicating the responses of the subjects. The issue discussed earlier is pinpointed after looking at the results. The results not only make it evident but also support my hypothesis of educating all sections of the society and not just the corporate employees. The following sections explain in greater detail the methods followed in conducting the survey and the observations made from the same.

RELATED WORK

Developing counter measures against cyber crimes has become the 'want' for everyone. The need for extensive browsing has developed over the years with all in-person transactions getting converted into online payments/shopping/playing etc. It is a human tendency to not just be eager to use the latest technology but also to be worried about keeping sensitive data safe.

Research done in the past shows an elaborate study of social engineering attacks, the risks associated with it and the reasons for rapid expansion of cybercrimes [4]. As explained by Heartfield in [6], various approaches have been made in the direction of understanding types of attacks, the schemes used to carry them out, types of victims the attacker chooses and the applicable counter measures to contain the attack once identified. Phishing is the most common attack that dupes millions every day. An extensive study [5], [11], [9] on what phishing is exactly, how it is orchestrated along with how various tools such as 'PhishGuru' have been developed and proved to be successful by designers has been discussed. On realizing the humans can indeed be the weakest link in the entire security design, efforts have been made after analyzing a bunch of call center employees [3] and a bunch of employees who use social media in their working environment [10], to propose models such as Social Engineering Attack Detection Model and Social Engineering framework for social media [13] that aids these users to identify malicious content on the internet.

After coming up with constructive measures to contain and curb these attacks, researchers have conducted audits [12] to understand how the organizations have implemented the security protocols designed and performed a thorough analysis on the ongoing issues that are still faced by users with respect to the usability of the security system [2].

Despite these efforts, the issue of usability and privacy still exists. There have also been studies determining the psychological factors of humans contributing to making security decisions [7]. It is sometimes the nature of human brain that forces humans to make certain decisions that can prove to be a potential breach. After analysis on humans, educating the naive users, the researchers even realized that humans probably aren't the weakest link [8] and probably usability is. In an attempt to make the system secure, designers often forget the naive audience. Not everyone has the knowledge of a security administrator in order to use the system correctly. Though user education methods are one of the ways to bridge the gap of knowledge between the end users and the developers, making an easy, readable and interactive user interface is also important. A small step down by the developers and a small step up from the users can prove to be of immense value to maintaining a secure system.

RESEARCH QUESTIONS

As explained above, the goal of this paper is to find out that though security mechanisms are in place for protecting the user against semantic attacks, then why hasn't the percentage of scams or social engineering attacks reduced by even a margin? It was found that no research was done to test the productivity of these measures. By the end of the discussion I hope to answer the following questions:

1. How effective are the user education methods such as user training or SEADM model on the organization's vulnerability to semantic attacks?

2. Have the user education methods really reached all sections of the human population?

3. Is there any research on how the user education methods are actually being employed?

METHODOLOGY

The aim of conducting this experiment is to analyze typical web page navigation patterns of users in general (skilled and unskilled) while conducting transactions online along with common errors made by them and then come up with suggestions to make certain security procedures invisible and the user interface more usable so that it reduces the critical decision-making load from the users. The agenda is to study user patterns by making them complete certain tasks like - booking a flight/holiday destination, downloading a software/movies/song, buying fashion goods, while monitoring them live via a video call (Zoom) where I request them to share their screen. This was a best attempt to come up with a live field study with participants wishing to participate from across the globe. The study was followed by a questionnaire focusing on some security specific questions. The questions were intended to learn the mental model of the users that make them take certain security decisions. Using the responses, common procedures can be pinpointed which can then be suggested to be automated by the designers.

Twenty subjects took part in the study and correct conclusions and accurate and pragmatic suggestions were drawn. It was decided to keep an open age group (as everyone uses the internet these days) ranging from 13 y/o to 55 y/o. No gender differentiation. But it was decided to avoid people working in the IT sector as there was a surety to get biased answers. So, subjects were picked from all other domains ranging from doctors to engineers to entrepreneurs to students (who again, do not belong to a computer science domain). A google form which included details like their age, occupation and a small

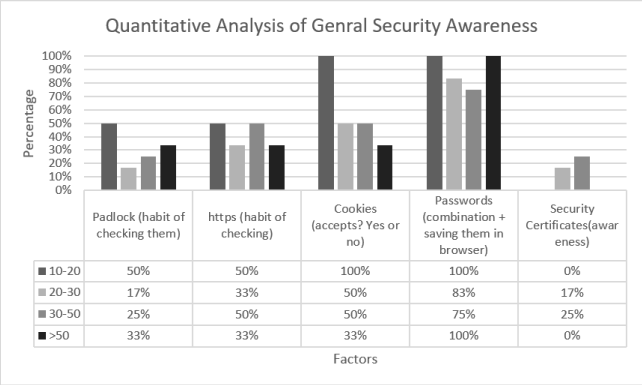
disclosure of what information they will be asked to share and for what purpose was circulated.

The main challenge faced during the conduction of the experiment was of time. Keeping a check of the time difference between two countries, coordinating with people sitting in India cost a lot of time. Though most of them were cooperative and active, I had limited hours to monitor them.

RESULTS

An online field study was conducted over an audience of twenty. The subjects having no background in computer science or information technology were chosen. The age of the subject varied from thirteen to over fifty. The subjects chosen were assigned certain day to day tasks (like – downloading a movie/song/software, booking a holiday destination, streaming a live match/race etc.). They were monitored online via a video conferencing platform and observations with respect to typical user patterns (such as which website they prefer, what are the usual trends in browsing etc.) were monitored during the conference. The entire process took approximately fifteen minutes. After the session, the subjects were asked to answer a few questions which determined their knowledge on security.

Various factors such as padlock checking, https, cookies, passwords, security certificates were checked. It was observed that most of the people didn't even know the meaning of these terms.



	Padlock (habit of checking them)	https (habit of checking)	Cookies (accepts? Yes or no)	Passwords (combination + saving them in browser)	Security Certificates(awareness)
10-20	50%	50%	100%	100%	0%
20-30	17%	33%	50%	83%	17%
30-50	25%	50%	50%	75%	25%
>50	33%	33%	33%	100%	0%

The graph clearly shows a very poor performance in the knowledge of security in naive users. It was also observed that most people know the constraints of setting up a password (because the websites impose them) but are unaware of the reason behind keeping the strong password. As a result, most of them have the same password with a very minor variation across many platforms. It was also observed that people tend to keep personal details in their password (such as spouses name/birth year etc.) so that it is easy for them to remember it.

Secondly, it was also observed that people know they shouldn't be accepting cookies because they are "bad". They were not aware of what cookies are and what they can be used for.

Thirdly, it was observed that people are always in a hurry to get their things done. By observing the manner in which they narrowed down the site for the task assigned, nobody spent more than five minutes for the task and that nobody researched or referred anything else before doing their task, it was concluded that people like completing their tasks head-on and hardly care about compromising their security because they are unaware of what is at stake and do not know the repercussions of their actions. They ended up creating unnecessary login accounts on various platforms because they wanted to get things done. Many of them claimed to save their card details online to save time.

Fourthly, it was also observed that people are unaware of browser cache clearing. When asked how often they clear their cache, 80 % of them replied saying they do it when their computers are "stuck" or are "slow". The subjects also made clear that they do not click on random links. Some of them said that they browse only those links which are "well-known" or those which are familiar to them.

Lastly the subjects were asked what they find most annoying while browsing. Almost 98 % reverted back by saying the advertisements and website redirection are somethings that are very annoying. They feel helpless when some ad pops up and sometimes distracts them to such an extent that it breaks their link, and they completely forget what they were browsing in the first place. These difficulties/concerns/common errors can be taken ahead as a future scope to make alterations in the current system designs. These observations can be marked as a trade-off between usability and security.

DISCUSSION

The experiment conducted aimed to determine the thought process of the users and their expectations out of the system. It also aimed at learning the typical human patterns of dealing with security decisions and coming up with suggestions to reduce the load of users. Various models have been proposed like the SEADM in [3] and SESM in [13] which can be used by the users to detect social engineering attacks. Though various such user education methods have been employed, the results obtained in the experiment clearly show a lack of knowledge. It has been observed that the users chosen did not belong to any organization and hence were the 'day-to-day' users.

A lot of research has been done on early detection of semantic attacks [6], checking the effectiveness of methods of early detection of semantic attacks [12] but there are no efforts made in making the day-to-day user alert and informed. People who do not belong to any organization aren't aware of semantic attacks, aren't aware of the precautionary measures that are to be taken. There is a desperate need to educate this section of the population. Various education programs can be employed by browser owners or advertisement boards which can make a naive user aware of the kind of attack he can be exposed to because people who aren't employed by an organization are unable to undergo training programs regarding awareness of semantic attacks.

On observing the movements of users on the browser, they clearly displayed a pattern of making security decisions which by the end of the experiment, was almost predictable. There are two observations made here -

- The users only care about completing the task and hardly bother about security as rightly said by Damilare D. Fagbemi in [1]

- The users are highly annoyed by the unnecessary advertisements and site re-directions.

The designers can take up these as enhancements to the current design of the system.

Though the research conducted is producing productive observations and conclusions, we cannot possibly draw a marker of feasibility of the suggestions made. If the enhancements suggested involve a lot of complicated implementations leading to a cascading effect, they will probably be dropped by the designers. Next, the adequacy of time allotted to conduct the research limited the window of responses. Also, there is no information on the scale of the population. By this I mean we have no knowledge of how much (how much percentage) this section of population (which was picked for the experiment) actually accounts for in the overall collective general population. If this population doesn't really form an integral part of the general population, the designer will probably drop alterations to the current design if the suggestions demand a major change in the system.

CONCLUSIONS

The threat to users is increasing day by day as technology is getting advanced and users lack the correct knowledge regarding security norms and precautions when using the internet. As everything has become 'one click' away, it has become easy for attackers to find discrepancies in the existing security system and breach the privacy of any individual. Thus, user education has widely gained its importance.

Though various efforts have been made by organizations in imposing user education, there is a certain section of population that has been left out. This population includes people who do not belong to any corporate organization, have retired from work or haven't begun working at all i.e., school students. My analysis shows that the internet is widely used by school students to complete projects, download study material/softwares or simply online gaming. People who do not work also use the internet widely to pay bills, shop online or simply browse a topic of interest. Research doesn't show any contribution on education methods employed on these people. My study was able to identify and highlight this stratum of population to researchers and was able to draw an insight into how common man needs to be educated about internet security and risks from which they are currently left out.

Therefore, the researchers can either employ specific user education methods on these users or can encourage the security developers to incorporate changes in the current security design in order to make it more interactive and safe for a naive audience.

Limitations and Future Work

As stated earlier, the users barely care about security and are always in a hurry to complete their task. If considered, these two observations convey a lot of information to the designer of the security system.

First, the designers can implement machine learning algorithms to learn a new user's pattern of browsing and can then use these patterns to come up with an enhancement in the UI that can guide the user to make security decisions. For example, if the algorithms learns that a particular user clicks on the first link of everything he browses, the designer can design a prompt for the user that pops up if the first link he is about to click on is malicious. Next, if the user is in a habit of creating multiple logins to get his work done and uses the browser to remember the logins for such unnecessary accounts, the designer can introduce methods in which the browser clears its own cache after a certain period of time.

To address the second observation, the ads and cookies can be used effectively to educate the users on semantic attacks. There are no measures taken by the browsers - like initiating obvious warnings to the user before he attempts to browse a malicious website or blocking malicious websites/redirecting the user to a safer website.

ACKNOWLEDGMENTS

I would like to thank my Professor Stacey Watson for constantly guiding me throughout the project. Her clear-cut guided procedure on how to go about each section in the paper helped me complete it. I would also like to thank my TA, Siddharth Das whose constant support in answering my concerns and questions helped me clarify various doubts. His insightful suggestions on certain approaches I took gave me a different angle of looking at things. Thirdly I would like to thank my parents who helped me come up with a framework as to how I should go about performing my study in such limited time frame. Last but not the least I want to thank my subjects, who diligently and honestly participated in my survey despite their hectic lives and schedules. Grateful to this strong support, I was able to complete my study.

REFERENCES

[1] 2019. *The Security We Need Designing Usable IoT Security by Damilare D. Fagbemi*. YouTube. https://www.youtube.com/watch?v=38uwvXN58Ko

[2] Hussain Aldawood and Geoffrey Skinner. 2019. Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet* 11, 3 (2019), 73.

[3] Monique Bezuidenhout, Francois Mouton, and Hein S Venter. 2010. Social engineering attack detection model: Seadm. In *2010 Information Security for South Africa*. IEEE, 1–8.

[4] Nabie Y Conteh and Paul J Schmick. 2016. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research* 6, 23 (2016), 31.

[5] Surbhi Gupta, Abhishek Singhal, and Akanksha Kapoor. 2016. A literature survey on social engineering attacks: Phishing attack. In *2016 international conference on computing, communication and automation (ICCCA)*. IEEE, 537–540.

[6] Ryan Heartfield and George Loukas. 2015. A taxonomy of attacks and a survey of defence mechanisms for

semantic social engineering attacks. *ACM Computing Surveys (CSUR)* 48, 3 (2015), 1–39.

[7] Ryan Heartfield and George Loukas. 2018. Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. *Computers & Security* 76 (2018), 101–127.

[8] Ryan Heartfield, George Loukas, and Diane Gan. 2016. You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks. *IEEE Access* 4 (2016), 6910–6928.

[9] Matthew L Jensen, Ryan Wright, Alexandra Durcikova, and Shamya Karumbaiah. 2020. Building the Human Firewall: Combating Phishing through Collective Action of Individuals Using Leaderboards. *Available at SSRN 3622322* (2020).

[10] Katharina Krombholz, Heidelinde Hobel, Markus Huber, and Edgar Weippl. 2013. Social engineering attacks on the knowledge worker. In *Proceedings of the 6th International Conference on Security of Information and Networks*. 28–35.

[11] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. 2010. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)* 10, 2 (2010), 1–31.

[12] Gregory L Orgill, Gordon W Romney, Michael G Bailey, and Paul M Orgill. 2004. The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. In *Proceedings of the 5th conference on Information technology education*. 177–181.

[13] Heidi Wilcox and Maumita Bhattacharya. 2016. A framework to mitigate social engineering through social media within the enterprise. In *2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA)*. IEEE, 1039–1044.