Research Hub Volume 5 Issue 11 (2019) eISSN:2180-0065

Threat in Computer Security Among the User in UiTM Puncak Perdana

Qkhairuel Shayidbullah Rosdi

Faculty of Information Management,
Universiti Teknologi MARA, Malaysia

Received: 27 June 2019 • Accepted: 21 October 2019

Absract. Computer is a very popular machine and also important communication tool all over the world. In this era, computer becomes very important for users which are including students, staff, lecturer and others. Computer not only functioned as their online communication but also a medium for data keeping and daily tools for work. Accommodate to the Internet world Stats: Usage and Population Statistic there are over 4 billion internet users all over the world and make the computer as a main medium for the access. It is because computer plays an important role in daily life the threat also expands as big as the importance's. In this research, it studies about the threat in computer security among the user in UiTM Puncak Perdana. This research also shows about the contributing factor and type threat engage with the user. In this research, we will distribute survey questionnaire towards the undergraduate students, staff and lecturer in the faculty of Information Management at the UiTM Puncak Perdana.
Keywords: computer, computer security, cyber security, threat

Introduction

PC is a well-known machine and furthermore imperative specialized instrument everywhere throughout the world. In this period, PC turns out to be critical for clients who are including understudies, staff, teacher and others. PC worked as their online correspondence as well as a mechanism for information keeping and every day instruments for work. Oblige to the Internet world Stats: Usage and Population Statistic there are more than 4 billion web clients everywhere throughout the world and make the PC as a principle vehicle for the entrance. It is on the grounds that PC assumes an essential job in everyday life the danger likewise grows as large as the importance's. In this exploration, it learns about the danger in PC security among the client. This examination additionally appears about the contributing element and type danger draw in with the client.

A threat, with regards to PC security, alludes to whatever can possibly make genuine damage a PC framework. A danger is something that could possibly occur, yet can possibly cause genuine harm. Dangers can prompt assaults on PC frameworks, systems and that's only the tip of the iceberg. Threats are possibilities for vulnerabilities to transform into assaults on PC frameworks, systems, and that's only the tip of the iceberg. They can put people's PC frameworks and business PCs in danger, so

vulnerabilities must be fixed with the goal that assailants can't penetrate the framework and cause harm.

Threat can incorporate everything from infections, Trojans, secondary passages to inside and out assaults from programmers. Regularly, the term mixed danger is progressively exact, as most of dangers include different endeavors. For instance, a programmer may utilize a phishing assault to pick up data about a system and break into a system. Based to the Internet World Statistics: Usage and Population Statistics, there are more than 4 billion internet users worldwide, which making the computer the main access medium for the usage. It is because computers play an important role in everyday life that the threat also expands as great as the significance.

Literature Review

Malware

One of fundamental assault or risk in PC security is malware. Malware is a paragliding term that portrays any malignant program or code that is hurtful to frameworks. Threatening, nosy, and intentionally awful, malware tries to attack, harm, or cripple PCs, PC frameworks, systems, tablets, and cell phones, regularly through fractional power over the activities of a gadget.

First paper that has been chosen is the marvel of information data loss and digital security issues in Ghana by Adu & Adjei (2018). This examination is planned to explore the mindfulness and arrangements of digital security inside Ghana's corporate associations. Expanding dependence on ICTs has made frameworks and administrations considerably more helpless. Particularly to the malware assaults and has opened the conduit to carry out genuine monetary wrongdoing. As indicated by Magele in 2015, the Internet has turned into a twofold - edged sword that offers open doors for people and associations while representing a danger of data security. About 1% of all messages sent in 2016 were basically pernicious assaults, the most noteworthy as of late (Global Cyber-Security Index, 2017).

Next is s study about Malware at its worst: death and destruction by Brody, Chang, & Schoenberg (2018). This article underscores on familiarity with malware however they may not know about the most hazardous type of malware which can cause physical mischief and even passing to individuals. This paper reason for existing is to reporting how programming can hurt individuals by assaulting present day frameworks that appear to be dismissed and under - investigated. By definition, malware a kind of short for malignant programming and is utilized to infiltrate and hurt the PC frameworks. At the point when it's come about malware, consideration generally attracted to cash based - related issues or absence of information get to. As of now, malware can assume responsibility for PCs, PDAs and e - business servers, and the product developer or programmer can likewise utilize it in various approaches to accomplish diverse objectives. A case of malware is a spyware. As indicated by Van Alstin in 2016, spyware is utilized consistently with adware to follow your web movement and afterward utilize that data to send adware back to your framework to lure you to buy the adulterated merchandise that the adware presents.

Using response action with intelligent intrusion detection and prevention system against web application malware is an article by Ammar Alazab, Hobbs, Abawajy, Khraisat & Alazab (2014). This paper means to moderate vulnerabilities in web applications; the most vital systems for security will be security identification and avoidance. The principle issue is the vulnerabilities of the web application. Next, a mix of a SIDS and an AIDS, to be specific the IIDPS, will be proposed. This paper displays a novel methodology by utilizing fluffy rationale to associate the IIDPS to a reaction activity. At last, utilize the hazard appraisal to decide an appropriate reaction. The finding is a mix of a Signature - based Intrusion Detection System (SIDS) and an AIDS - based Anomaly - based Intrusion Detection System (IIDPS).

Pishing

Other primary assault or risk in PC security is phishing. Phishing is a kind of social designing assault frequently used to take client information. Phishing likewise take the data with respect to login certifications and charge card numbers. It happens when an aggressor or taking on the appearance of a confided in element. This is when then the aggressors hoodwink an injured individual into opening an email, text, or instant message. In view of the writing audit to help this announcement there are many article and research paper that can be utilized.

The first articles regarding the phishing attack is by Curtisa, Prashanth Rajivanb & Jonesa, Gonzalezb (2018) which is phishing attempts among the dark triad: Patterns of attack and vulnerability. This study shows the connections between three identity qualities, Machiavellian, narcissism, and phishing and psychopathy exertion, assault achievement, and end - client phishing affectability. In two phases, members were enrolled. Discoveries recommend that the scores of aggressors are identified with the exertion they made. To compose a phishing email related with expanded phishing with more elevated amounts of Machiavellian aggressor.

André Lötter & Lynn Futcher (2015), an article about phishing which is a framework to assist email users in the identification of phishing attacks. The primary goal of this article is to propose a system to address the issue that email clients are not very much educated or helped by their email customers in recognizing potential phishing assaults, along these lines imperiling their own data. Thusly, this paper tends to both the human shortcoming and the product - related issue of email customers that don't outwardly help and guide clients through the UI. "Social Phishing" characterizes phishing as "a type of social designing in which an assailant endeavors to gain touchy data from an injured individual deceitfully by mimicking a confided in outsider" (Jagatic et al., 2005). This paper contends that email clients should utilize input instruments to exhibit security - related perspectives to their clients so as to make them mindful of the phishing assault attributes. It exhibits a system to help this contention to help email clients distinguish phishing assaults.

The next study chosen is persuading end users to act cautiously online: a fear appeals study on phishing by Jurjen Jansen & Paul van Schaik (2018). The reason for this paper is to test the hypothesis of assurance inspiration to decrease the danger of phishing assaults with regards to fear advance intercessions. Moreover, it has been tried to what degree the model connections are proportional as far as dread and time. Phishing is considered incredibly risky to web clients (Arachchilage et al., 2016) and

is a worldwide issue (APWG, 2015) for different areas, for example, retail and banking. Thought of online data - sharing conduct is essential since it encourages phishing assaults event and achievement. The outcomes give more understanding into essential factors that should be tended to in planning preventive measures to decrease phishing assault achievement. The examination found that associations with the PMT display are in the phishing area. The most vital indicators of security inspiration were self - viability and dread, and the consequences of the model were commonly proportional crosswise over conditions and after some time.

Online Fraud/Cyber Scam

Cybercrime causes financial losses that are boggling to the order of trillions of dollars around the world. Unfortunately, the vastness of this crime and its effects is not known to most individuals and organizations. Many attempts have been made to control this rapidly spreading threat of cybercrime at global level, due to a variety of reasons it has borne little results.

The first study about computer fraud or cyber fraud is Cybercrime: a portrait of the landscape by Furnell & Samantha Dowling (2019). The target of this paper is to inspect current proof in regards to the scale and effect of cybercrime, including distinctive ways to deal with issue definition and estimation. The cybercrime issue is certifiably not another one, and for well more than three decades related occurrences have happened in different structures. Revealing from the digital security industry recommends that the issue was not static – the scale and expansiveness of some specific types of digital - assault announced by industry seems to have expanded as innovation use has turned out to be increasingly across the board and its criminal potential has turned out to be all the more generally perceived. The paper demonstrates that cybercrime exists in various measurements, with comparably differed expenses and damages. There is likewise a feeling that, the same number of wrongdoings can possibly have an innovation part, the "digital" name will turn out to be to some degree repetitive.

The next study is Predicting susceptibility to cyber-fraud victimhood by Whitty (2019). This paper is purpose to develop a theoretical framework for predicting sensitivity to the victimhood of cyber- fraud. Digital fraud are any sort of trick that misuses email, Instant Messenger, long range interpersonal communication destinations that trap individuals out of cash (Whitty, 2015a). The precedents incorporates outside lotteries and sweepstakes in which the unfortunate casualty trusts that they have won cash from a lottery and are advised to pay a charge to discharge the assets, 419 tricks are pre - expense extortion, in which exploited people trust that they will make an extensive fortune for a little measure of cash and sentimental tricks taken in by a phony web based dating persona in which the injured individual sends the ' counterfeit persona'. The last soaked model uncovered that the forecast of unfortunate casualty hood should consider mental and human science - statistic qualities and online routine exercises. As indicated by the theories, digital - misrepresentation exploited people were bound to be more established, score high on direness and sensation - looking for rash measures, score high on addictive measures, and take part in progressively visit routine exercises that put them at high danger of defrauding. There was little distinction between coincidental and rehashed digital misrepresentation exploited people.

Next article is entitled as online fraud offending within an Australian jurisdiction by Bolimos & Raymond Choo (2017). The purpose of this paper is to determine the level of offending online fraud within an Australian jurisdiction and how best to use resources to combat it. There are a number of categories of online fraud, including email fraud, online dating fraud and sales fraud. Email frauds can include phishing such as fake emails from banks, credit companies and other companies seeking personal information and advance expense misrepresentation. Web based dating cheats are those when exploited people are focused through dating locales or different methods and baited into a "relationship" including increasingly more cash being sent by the unfortunate casualty to "help" them accomplish an objective? Deals extortion includes individuals selling or acquiring products. The either at costs that are unrealistic or through escrow firms that appear to be real yet have been set up legitimately by the trickster itself utilizing self \-trotted manipulative procedures. In spite of the fact that the periods of online extortion unfortunate casualties contrasted, there was a somewhat higher shot that a more established individual from the populace would succumb to a guilty party than a more youthful individual. On the off chance that the absolute number of members around there was likewise high, the quantity of a specific sexual orientation detailing an occurrence of cybercrime in a given zone might be higher. More seasoned unfortunate casualties were bound to lose to online misrepresentation bigger measures of cash. Likewise, it was discovered this expanded to over 80% when the non-sex recognizable information were evacuated.

Misuse and Spam

Spam is newsgroup posts by electronic junk mail or junk. Some people define spam as any unsolicited email even more generally. However, if a brother who has been lost for a long time finds your email address and sends you a message, it could hardly be called spam even if it is not requested. Real spam is usually email advertising that is sent to a mailing list or newsgroup for some product.

The first study is the article about Spam classification: a comparative analysis of different boosted decision tree approaches by Shrawan Kumar Trivedi and Prabin Kumar Panigrahi (2018). This paper aims for introducing near investigation among various choice tree classifiers incorporates choice tree with or without various boosting calculations, for example, AD tree, choice stump and REP tree. One of the email use issues is spontaneous messages sent over the web, which is called spam. Substances commonly use spam to send messages for publicizing, phishing, or getting to data to countless clients. Organizations can acquire tremendous cash by supporting promotions through e - mail spam. Therefore, when email clients get spontaneous messages that can be destructive and undesirable, they face distinctive kinds of issues. The aftereffects of this investigation demonstrate that the REP tree gives superior precision as the second - best entertainer with the AD tree positioning without boosting. Choice stump is observed to be this present examination's classifier under execution. On the off chance that the measurements are taken together false positive rate and exactness of execution, both AD tree and REP tree were found to play out a successful arrangement task.

Next is the study regarding misuse and spam is investigating employee harassment via social media Taylor, Haggerty, David Gresty, Criado Pacheco, Berry & Almond

(2015). The target of this paper is to analyse the procedure of representative provocation examination through internet based life to grow best practices to help associations all the more viably direct such examinations. Kaupins & Park (2011), said corporate interpersonal interaction locales could give critical chances to data sharing to representatives and bosses. Van Laer (2013), in any case, remarked that maltreatment of social stage as digital provocation could affect clients of online networking, for example, enthusiastic misery. Associations might not have powerful techniques for examining abuse of online networking, when all is said in done, and specifically badgering of representatives through web based life.

Hacking And Hijacking

Because of rising digital dangers and expanding digital hacking exercises, the digital security industry has developed quickly as of late. Rising innovation investigates features the dangers and some of the time dismisses the potential commitment to digital security. Hacking more often than not alludes to exercises went for trading off advanced contraptions, for example, cell phones, PCs, tablets, and even entire systems. PC commandeering alludes to the demonstration of adjusting or changing PC programming and equipment to accomplish an objective considered to be past the first target of the maker.

The first paper that discuss about hacking is Foresight of cyber security threat drivers and affecting technologies by Raban & Hauptman (2018). The point of this investigation is to lead a moderately adjusted long haul premonition concentrate to create real drivers of risk and to distinguish rising advances that are probably going to affect digital security resistance and assault capacities. Because of rising digital dangers and expanding digital hacking exercises, the digital security industry has risen quickly lately. Evoke real drivers of risk and recognize developing innovations that are probably going to affect digital security essentially adversely or emphatically. The principle device utilized in this examination is an online overview of point specialists assessing developing dangers and the potential effect of a few rising advancements on digital barrier abilities of a few rising advances. A specialist overview demonstrates that digital flexibility, homophobic encoding, and square chain ought to be viewed as advances that for the most part make a huge commitment to safeguard capacities. Then again, the Cloud figuring, bio hacking and human machine interface and self-governing advances make a commitment primarily to capacities of attack.

The next study about computer fraud or cyber fraud is Cybercrime: a portrait of the landscape by Furnell & Samantha Dowling (2019). This paper objective problem and finding can be refers at 2.6 cyber fraud. This paper not only tells us about cyber fraud or also known as cyber scam but the content also shows us about computer or cyber hacking.

Cyber Terrorism

The following study or paper in regards to these issues is tension about computerized security and fear based oppression, and backing for counter-dread measures. Gallova, Palasinski, Shortland, Humann & Grieve (2018). This paper target issue and finding can be alludes at 2.4 abuse and spam in the digital world. This paper enlight-

ens us regarding spamming issues as well as shows us about PC or digital fear based oppression.

First study regarding these issues is anxiety about digital security and terrorism, and support for counter-terror measures. Gallova, Palasinski, Shortland, Humann & Grieve (2018). There is main concern that accessibility of interactive extremist content may increase radicalization potential (McGilloway et al., 2015).This is of developing concern given that in certifiable fear based oppressor assaults or endeavors online radical guidelines are frequently refreshed ; Edwards & Gribbon, 2013 ; Jackson & Loidolt, 2013 ; Lemieux et al., 2014). As indicated by Von Behr et al. (2013), the job of the web in radicalization was inspected and 15 instances of fanatics who utilized the web to have and increase radical data and spread their fanatic perspectives were distinguished. Research 1 proposes that while tension about computerized security frameworks, information assurance and long range interpersonal communication locales was anticipated decidedly by right - wing tyranny, nervousness about person to person communication was additionally anticipated contrarily by time spent on the web. Research 2 demonstrates that nervousness about residential fear mongering was a negative indicator of time spent on the web. Research 3 demonstrates that the most grounded positive indicator for all help is the measures were conservative tyranny and national character pursued.

The next study about cyber terrorism is the paper towards a framework for the potential cyber-terrorist threat to critical national infrastructure by Abdulrahman Alqahtani (2015). The aims behind this paper is to clarify that digital - watchfulness can prompt a few negative outcomes, including the potential for framework misuse, undermining the authenticity of popularity based frameworks, and unbalanced, not really viable disciplines. The security of states has been compromised by numerous occasions and risks. These dangers caused serious life misfortune, sickness spread, wounds, demolition of open and private property, relocation of tremendous quantities of individuals and monetary misfortunes. Global and neighbourhood political turmoil and later innovative advancements are components that would build the seriousness of dangers to national security (Inoguchi, 1996). The principal investigate, as a subjective exploratory examination, gives as a quantitative corroborative investigation a rich arrangement of information that gives the premise to the advancement of the second examination. It gives a superior hypothetical comprehension of the potential danger to Saudi national security from digital and customary fear based oppression in the past subjective investigation of the specialist. Be that as it may, it has additionally prompted the advancement of the calculated structure and the suspicions for the examination's second stage.

Analysis of Review

Based on previous study computer security or cyber security, cybercrime and cyber threats have caused a great deal of damage to individuals, private organizations and even the government today. In order to prevent and protect data from such attacks, cybercrime detection methods and classification methods have developed varying levels of success. However, the study shows that many countries still face this problem today, and over the years, the United States of America leads with maximum damage due to cybercrimes. According to the recent survey, 2013 saw the monetary damage of almost 781.84 million dollars in the United States. Furthermore, there are

also some case studies related to cybercrimes and cyber threats this include phishing, malware, hacking, fraud and others.

Table 1. Analysis of Review

Author	MALWARE	PISHING	CYBER FRAUD	MISUSE AND SPAM	HACKING AND HIJACKING	CYBER TERRORISM
Adu & Adjei (2018)	/					
Abdulrahman Alqahtani (2015)				/		/
Curtisa, Prashanth Rajivanb, Jonesa & Gonzalezb (2018)		/				
Raban, Hauptman (2018)					/	
Gallova, Palasinski, Shortland, Humann & Grieve (2018)						/
Lötter & Futcher (2015)		/				
Brody, Chang & Schoen-berg (2018)	/					
Paul Van Schaik (2018)		/				
Shrawan Kumar Trivedi & Prabin Ku-mar Panigra-hi (2018)				/		
Furnell, Dowling (2019)	/		/		/	
Aisha Aseeri					/	

& Omaimah Bamasag (2016)						
Whitty (2019)			/			
Bolimos & Raymond Choo (2017)			/			
Alazab, Hobbs, Jemal Abawajy, Khraisat & Mamoun Alazab (2014)	/					
Taylor, Haggerty, Gresty, Pacheco, Berry & Almond (2015)				/		

Based on the table 1, we make an analysis for conceptual framework. There are many threats regarding technology especially related to the topic computer security or also known as cyber security. Based on the analysis, it showed that the most focus study is on the malware attack, malware seeks to invade, damage, or disable computers meanwhile even through there are growing concern given for this issues about online terrorism and extremist, this limitation for the threats.

Conclusion

In conclusion, the main purpose of this study is to provide the threats faced by the world of technology, especially in computer or also cyber security. . Researchers want to give a little awareness especially in dedicating to people who involved directly in managing technology regarding the computer security. It is because nowadays, we did not alert the bad impacts and lost these threats can bring to any organization, users and civilian. Through this research, researchers want to give the awareness to the world of computer security especially to the threats in early stage and also as introduction.

References

Kofi Koranteng Adu, Emmanuel Adjei, (2018) "The phenomenon of data loss and cyber security issues in Ghana", foresight, Vol. 20 Issue: 2, pp.150-161, https://doi.org/10.1108/FS08-2017-0043

Abdulrahman Alqahtani, (2015) "Towards a framework for the potential cyber-terrorist threat to criticalnational infrastructure: A quantitative study", Information & Computer Security, Vol. 23 Issue: 5, pp.532-569, https://doi.org/10.1108/ICS-09-2014-0060

Shelby R. Curtisa, Prashanth Rajivanb, Daniel N. Jonesa, Cleotilde Gonzalezb,(2018) "Phishing attempts among the dark triad: Patterns of attack and vulnerability", Computers in Human Behavior. (2018), pp.174-182, http://dx.doi.org/10.1145/2063176.2063197

Mark Taylor, John Haggerty, David Gresty, Natalia Criado Pacheco, Tom Berry, Peter Almond,(2015) "Investigating employee harassment via social media", Journal of Systems and Information Technology, Vol. 17 Issue: 4, pp.322-335, https://doi.org/10.1108/JSIT-03-20150022

Yoel Raban, Aharon Hauptman, (2018) "Foresight of cyber security threat drivers and affecting technologies", foresight, Vol. 20 Issue: 4, pp.353-363, https://doi.org/10.1108/FS-02-20180020

Viktoria Gallova, Marek Palasinski, Neil Shortland, Michael Humann, Lorraine Bowman Grieve, (2018) "Anxiety about digital security and terrorism, and support for counter-terror measures", Safer Communities, Vol. 17 Issue: 3, pp.156-166, https://doi.org/10.1108/SC-022018-0007

André Lötter, Lynn Futcher, (2015) "A framework to assist email users in the identification of phishingattacks", Information & Computer Security, Vol. 23 Issue: 4, pp.370-381, https://doi.org/10.1108/ICS-10-2014-0070

Richard G. Brody, Harold U. Chang, Erich S. Schoenberg, (2018) "Malware at its worst: deathand destruction", International Journal of Accounting & Information Management, Vol. 26 Issue: 4, pp.527-540, https://doi.org/10.1108/IJAIM-04-2018-0046

Jurjen Jansen, Paul van Schaik, (2018) "Persuading end users to act cautiously online: a fearappeals study on phishing", Information & Computer Security, Vol. 26 Issue: 3, pp.264276, https://doi.org/10.1108/ICS-03-2018-0038

Shrawan Kumar Trivedi, Prabin Kumar Panigrahi, (2018) "Spam classification: a comparative analysisof different boosted decision tree approaches", Journal of Systems and Information Technology, Vol.20 Issue: 3, pp.298-105, https://doi.org/10.1108/JSIT-11-2017-0105

Steven Furnell, Samantha Dowling, (2019) "Cyber crime: a portrait of the landscape", Journal of Criminological Research,Policy and Practice, Vol. 5 Issue: 1, pp.13-26, https://doi.org/10.1108/JCRPP-07-2018-0021Permanent link to this document:https://doi.org/10.1108/JCRPP-07-2018-0021

Aisha Aseeri, Omaimah Bamasag, (2016) "Achieving protection against man-in-the-middle attack inHB family protocols implemented in RFID tags", International Journal of Pervasive Computing and Communications, Vol. 12 Issue: 3, pp.375-390, https://doi.org/10.1108/IJPCC03-2016-0015

Monica T. Whitty, (2019) "Predicting susceptibility to cyber-fraud victimhood", Journal of Financial Crime, Vol. 26 Issue: 1, pp.277-292, https://doi.org/10.1108/JFC-10-2017-0095

Ioannis A. Bolimos, Kim-Kwang Raymond Choo, (2017) "Online fraud offending within an Australianjurisdiction", Journal of Financial Crime, Vol. 24 Issue: 2, pp.277-308, https://doi.org/10.1108/JFC-05-2016-0029

Ammar Alazab, Michael Hobbs, Jemal Abawajy, Ansam Khraisat, Mamoun Alazab, (2014) "Using responseaction with intelligent intrusion detection and prevention system against web application malware",Information Management & Computer Security, Vol. 22 Issue: 5, pp.431449, https://doi.org/10.1108/IMCS-02-2013-0007