ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 7, Issue 4, pp: (114-117), Month: October - December 2019, Available at: www.researchpublish.com

Cybersecurity Awareness for Parents

Manus Naknawa, Jamaludin Ibrahim

Faculty of Information and Communication Technology,
International Islamic University Malaysia

Abstract: **We are currently living in an age, where the use of the internet has become second nature to millions of people (E.Kritzinger, S.H. von solms, 2010). People should know the cybersecurity awareness side by side with technology. Also, when we learn about Cybersecurity awareness it will come with Cybersecurity threats. the cybersecurity threat has a lot of from, maybe come from Malware or hacker themselves. Therefore, we need to know which form of cybersecurity threat is trending right now and how many forms of cybersecurity threats are might happen to our life. Moreover, how do we prevent or protecting our children and start learning about this situation, this paper will provide some tips to start preventing our children away from cyber threats.**

Index Terms: **Cybersecurity, Cybersecurity Threat, Parents, Children.**

I. INTRODUCTION

The era of the internet, everyone can access it every part of the country and the world. Therefore, it cannot be avoided that the risk will increase in the cyber world, especially right now everyone can buy a smartphone. Nearly two-thirds of Americans now own a smartphone (Pew Research Center 2015). Constant online presence brings both developmental benefits and also a number of new risks (Livingstone S, Haddon L, G€orzig A, Olafsson K. 2010). Parents should study and pursue a cyber world all the time due to in the cyber world when something happens it happening very fast and widespread. The duty of parents are protection, teaching, and prevention of the children away from cybersecurity threats. To learn how to prevent yourself (Parents) and children are not that hard. Moreover, 95 percent of all security incidents involve human error. The most prevalent mistake? Double clicking on an infected attachment or unsafe URL. Other common errors include lack of patching, using default user names and passwords and easy-to-guess passwords, lost laptops and mobile devices, and inadvertent disclosure of sensitive information by use of an incorrect email address (Cyber security Intelligence Index 2014).

II. PURPOSE OF THE PAPER

The purpose of this paper is to describe meaning of the topic and genre of a cybersecurity threat. Also, describe how to protect children from it. Aforementioned at the beginning, when we perceived the threat and genre of them. Then, our awareness will occur. Moreover, this paper also describes the cybersecurity threat that parents should special aware of due to the threat easily come to children or have been tricked.

III. WHAT IS CYBERSECURITY AWARENESS

Cybersecurity means all necessary process or action to eliminate all of the risks of an organization and damage that affect information security in every type of form. including preventing crime, attack, sabotage, espionage, and various mistake, by considering the basic elements of information security or CIA (Confidentiality, Integrity, Availability). Awareness means “stimulates and encourages those being trained to take care about information security and to continually remind them of important security practices” (EC-Council Official Courseware 2015). Cybersecurity awareness is all about conveying information and best practices to specific target groups. Cybersecurity awareness programs address how and what sorts of materials and tools can be used to convey messages and that make such programs successful and impactful or failures. It is the multidimensional structure of an awareness program itself that makes people interpret it differently at various levels. Therefore, understanding what constitutes effective cyber security awareness is imperative (Zahri Yunos, Ramona Susanty Ab Hamid, Mustaffa Ahmad 2016).

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 7, Issue 4, pp: (114-117), Month: October - December 2019, Available at: www.researchpublish.com

IV. WHAT IS CYBERSECURITY THREAT

In the age of everything is cyber, children cannot be avoided it. Also, cybersecurity threat cannot be avoided either. somehow the threats will come, it is a matter of time. The cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber-attacks include threats like computer viruses, data breaches, and Denial of Service (DoS) attacks (Hugh Taylor, 2018). There are a lot of threats like this what are parents should do?

V. CATEGORIES OF CYBERSECURITY THREAT

There are two categories of cybersecurity threat 1. Malware 2. Attack. Malware can separate in two type 1. Propagation (Distribution method) 2. Payload (Action to the system). It is not necessary that Malware can only do one thing, some of them can do a lot of things.

A. Malware (Propagation)

VIRUS: Malware that parasitic in a program, active when a program is running, propagation by user action (Ex. Click to start a program) then will be infected and propagating to next computer or else. WORM: malware that can spread by itself, User doesn't have to action. For example, when plug in USB drive, Worm can access to PC by itself no need action from user. TROJAN: Malware which parasitic inside the device and waits for conduct something, Trojan usually does not have propagation to other devices by user or user device but might parasitic in a program that seems a good program (ex. music program).

virus, worm, trojan when the device was infected by them, it can harm to device in many forms, it can be damaged to information (assets) or even hardware.

B. Malware (Payload)

SPYWARE: Point of spyware is spying on user. For example, Financial information, Email, keyboard typing (Keylogging). ADWARE: keeps showing an advertisement in various ways. For example, change the default search engine of browser, pop-up ads, or changed ads on the website to their own ads. ROOTKITS: malware that will elevate to who using it can have the same privilege as an admin of the system. BOTNETS: Botnets are computer networks (or other devices) which infected by malware inside, using a host resource to do something. For example, Distributed Denial of Service (DDoS), bitcoin mining, Spam sender, Brute force attack, and so on. the system that has been in botnets are called Zombie System. BACKDOORS: path to the system by intentionally left it behind for access to system without using normal method. For example, the programmer left Backdoors for fixing bug later, or hacker was hacked to system and open Backdoors for next time. LOGIC BOMBS: malware that waiting for some condition. For example, waiting for a date to action. RANSOMWARE: In 2018 was very high trending of this malware, it is malware that ransom by locked computer or encrypt data until the victim pays it.

C. Attack

There are a lot of Attack type but this paper will only tell Attack that happen frequently. DoS/DDoS: DoS happens when an attacker sending tons of request to a server for trying to keep a server busy until a server cannot answer a request. But DoS can prevent by block some of an IP address. Therefore, to penetrate this prevention, DDoS will have a role in this, DDoS using Zombie System in Botnets to prepare the attack. A trending method is sending a request to the server but by spoofing IP and then fool the server to send a request back to the victim, this method called Smurf Attack. MAN-IN-THE-MIDDLE (MITM): MITM is a hacker that stay in the middle between user and server. therefore, a hacker will able to see all data. EVIL TWINS: The attacker will set a new WiFi name looks familiar to an authentic wifi provider. For example, hackers set SSID (name of WiFi) "Airport_WiFi" look like the real one, when people connect to the fake WiFi they can easily stole the data. PHISHING: the attacker will send an Email to the user by imitating like a real one. For example, an attacker sending imitating email that likes an email from bank tells that "your account has been compromised, click this link to change password" when the user clicks a link, the user has to fill username and password to log in if the user filled, Username and password will be collected. PHARMING: pharming is a fraud website that looks like a target website (like bank website) and then the attacker will use some method to redirect the user to this fraud website without notice. Moreover, phishing is the one method but still, there are a lot of method. TYPOSQUATTING (URL HIJACKING): made a website that looks like a target website and then waits for users to fill the wrong website.

For example, the user tried to type www.aliexpress.com but missed type to www.alixpress.com. HOAX: Hoax is fake news. For example, tells the user that some file in your device is dangerous, delete as soon as possible. But when deleted some bugs are happens.

The reason why this paper tells a lot about all types of malware, due to there is a record from 2018, 34.4 percent came from malware and next is Account hijacking 18.2 percent, record has been collected a total of 1337 events (Hackmageddon, 2019).

VI. CYBERSECURITY THREATS FACED BY CHILDREN

The Internet can be a risky neighborhood for children. From cyber-predators to social media posts that can cause issues to them later in life, the risks can be frightening. Children may also accidentally reveal their families to online dangers. for instance, by inadvertently downloading malware that could give cybercriminals access to their parents' bank account other sensitive information. Ensuring children on the Internet is most importantly a matter of awareness, realizing what risks lurk how to safeguard against them. Cybersecurity software can help ensure against certain dangers, yet the most significant security measure is communicating with your children. There are seven risks that children often face in online. (1) CYBERBULLYING: According to Internetsafety101.org, 90 percent of youngsters who participate in social media have overlooked bullying they've seen, and 33 percent have been victims of cyberbullying themselves. Social media and online games are the present virtual play area, and that is the place much cyberbullying happens. For instance, children can be taunted in social media exchanges. Or then again, in online games. (2) CYBERPREDATORS: Sexual and other predators can stalk kids on the Internet, exploiting children's honesty, abusing their trust and, maybe, luring them into very dangerous personal encounters. (3) REVEAL PRIVATE INFORMATION: Children do not yet comprehend social limits. They may post individual data online, for instance in their social media profiles that ought not to be out in the public. This may be anything from pictures of awkward personal moments to their street numbers. (4) PHISHING: (You can find meaning of it on sub-topic “CATEGORIES OF CYBERSECURITY THREAT”). (5) SCAMS: Children may succumb to scams that offer things they may prize, for example, free access to online games. children are easy marks for scams due to they have not yet figured out how to be vigilant. (6) ACCIDENTALLY DOWNLOADING MALWARE: Cybercriminals frequently trick people into downloading malware. Phishing is one such trick, but there are others such as convincing victims to download purported games that can be especially beguiling to children. (7) HAUNTING POST FROM A PREVIOUS TIME: The Internet doesn't have an erase key. Anything your child puts online is almost difficult to expel later. But teenagers, in particular, are not thinking about how a future boss or, one day, a prospective spouse might respond to "amusing" images or other personal content that they post to their social media profiles or other websites.

VII. HOW SHOULD PARENTS TREAT THEIR CHILDREN

Parents are an important role who will teach the children. There is a record from research that tells us, 69% of parents are supervising their child's computer time while 31% did not supervise their child at all (Wanda Cassidy, Karen Brown, Margaret Jackson, 2012). there are tips from author. (1) The parents should get used to the internet and technology, just get used to it do not have to be an expert. For example, know tools and websites that are highly trending in children, and then find good side and bad side or find any risk from tools and websites, threats usually have a similar pattern. In games might have bullying between players or social media might have enticement. (2) Teach them about security from the beginning, a lot of parents cannot decide when they are going to let children using technology (smartphone, computer, and so on), but if the kid is under parents notice and if parents know what are they doing, it is enough but don't forget to teach them about security and (3) talking with them about social media privacy, social media privacy might easily be called “ limiting the scope of people able to see pictures, videos, and activities”. the essence of this is criminals usually collecting our information by social media like what are we doing? where are we? or lure the kid going to somewhere they want. Therefore, limiting the scope of people to see our activities need to be appropriate. (4) make sure all devices are secure and protected, after getting used to the internet and technology can be able to guide children to knows security and privacy, the device needs to secure too, with parental control apps, for example, that’s possible. This technology allows parents “safeguard children on smartphones and tablets in this complex digital era”, while also preventing them from racking up an expensive bill with in-app purchases.

VIII. CONCLUSION

Cybersecurity awareness is an important thing that everyone should pay attention, it does not necessarily only parents. From statistics, Malware is the number one from the cyber world in 2017 and 2018, 2019 might still remain number one. Parents should pay attention and teaching children to know about the threat from the cyber world and sometimes lots of things that happen in the cyber world also relevant or connect to the cyber threat. For example, cyberbully there is a connection between cybersecurity and cyberbullying, many people might not make a connection between these two events (Marissa Bergen, 2018). 4 tips are useful for starting a cybersecurity awareness.

REFERENCES

[1] Kritzinger, E., & Solms, S. H. Von. (2010). Cyber security for home users : A new way of protection through awareness enforcement. *Computers & Security*, *29*(8), 840–847. https://doi.org/10.1016/j.cose.2010.08.001

[2] Pew Research Center. (2015). "The Smartphone Difference". Available at: http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/

[3] Livingstone S, Haddon L, G€orzig A, Olafsson K. 2010. Risks and safety for children on the internet: the UK report. Politics, 6: 1.

[4] Prey Nation. (2018). "What are cyber threats: How they affect you and what to do about them". Available at : https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/

[5] HACKMAGEDDON. (2018). "2018: A year of cyber attack". Available at: https://www.hackmageddon.com/2019/01/15/2018-a-year-of-cyber-attacks/

[6] Cassidy, W. (2012). " MAKING KIND COOL ": PARENTS ' SUGGESTIONS FOR PREVENTING CYBER BULLYING AND FOSTERING CYBER KINDNESS *. 46(4), 415–436.

[7] Incyberdefense. (2018). "Cyber security and Cyberbullying: There is a connection". Available at: https://incyberdefense.com/editors-picks/cyber-security-and-cyberbullying-there-is-a-connection/

[8] EC-Council Official Courseware. Certified Chief Information Security Officer, 2015.

[9] Yunos, Z., Susanty, R., Hamid, A., & Ahmad, M. (2016). Development of a Cyber Security Awareness Srategy Using focus Group Discussion. 1063 – 1067.

[10] Security Intelligence. (2014). "Cyber Security Intekkigence Index 2014". Available at: https://securityintelligence.com/cybersecurity-awareness-is-about-both-knowing-and-doing/