GRADUATE SUCCES ATTRIBUTE

1st INDIVIDUAL ASSIGNMENT

TOPIC: PRIVACY INVADE AND HOW WE CAN BE INVISIBLE IN THIS MODERN WORLD

PREPARED BY: MUHAMMAD FIKRI BIN ABDULLAMIN

MATRICS NO: A19EC0096

DATE:27 SEMPTEMBER 2019

PREPARE FOR: DR MUHAMMAD ABD HADI BIN BUNYAMIN

PRIVACY INVADE AND HOW WE CAN BE INVISIBLE IN THIS MODERN WORLD

“My wife knows where the photos came from and why they were taken. And they were not meant to be distributed,” said the 40-year-old artiste when met a launch of his new album Rojak. “Nobody should judge me. I didn’t distribute them and I have no idea who got hold of them,” (Alhamzah, T, 2019, p.1) said the Ragaman singer Faizal Tahir who shocked that the nude photos of him were circulating on social media.

Privacy are precious in everyone life. It a personal space that keeps us apart from the busy world. According to Parent, W.A. (1983) privacy can be defined as the condition of not having undocumented personal information about oneself know by others. Of course, It totally rely on a person to decide which information are personal and which one is not as different people has their different meaning of information. After all, we all will come up with the same conclusion, we have to protect our privacy because have the right to do so. And privacy does not just affect our right, it is a human right. In fact, privacy is recognized as a fundamental human right.

In Malaysia, it’s pretty common that our privacy has been invade once regardless whether is something that we aware or not. This is because the community think privacy is unimportant matter that has not to worry about. This is what they thought until their private space being invade, when that time happens, it’s already too late to turn things around. It’s wise for us to take a precaution step to avoid our privacy being breach by unwanted person. Taking care of your privacy not only will help you to secure your private life, it also will help you to avoid being one of the victims of popular crime right now which is scams.

Before we proceed to the precaution steps, let’s take a look of what the unwelcome agencies or people can do with our privacy data and see how dangerous it can be. For example, let’s say you work at big company and you love your jobs there. You have been working on this upcoming mega project. Your friend, let’s say it is your best friend, somehow know about the project. Maybe he secretly sneaking your phone when you not around. One day, you have been arguing with him because he doesn’t pay your money back. To revenge on that matter, your friend sabotages your project and you been fire from the company as the result of that. Well that one of the scenarios. How about the other agencies?

Third party agencies usually will spy on the information that you enter on the internet to help with their advertisement. Although, it may sound harmless, it could be annoying for certain people as Ads keep showing on their browser. There also another party call Experian and Axiom. It is Basically a data warehouse that collect as much data as possible about a person and sell it. (Mitnick, K.&Vamosi ,R., 2017). The way they collecting your data is by returning an additional script or image every time you search on your browser. Your browser will convert the host name into numerical IP address first and the request information from that site. (Mitnick, K. et al., 2017) The site will send back the information to your browser back including the addition script. This information is what you see on your screen, doesn't matter whether it is image or a line of paragraph. In contrast to that, the additional script will inform other parties that you have been on this site. Now everyone know that you have been on that site.

Sometimes, it seems reasonable on why these parties trying so hard to mine as much data as possible to help the growth of their companies and thus improve the economy. If you notice, every time you search something on Lazada, let's say a monitor, there will be ads pop out on your social media about the promotion for the monitor. Usually the ads will show a limited time promotion like 50% discount or buy 1 free 1 or whatever that attract you to click it. In this way, you will be benefit from the data mining as you get the monitor you want for half of the price on the market. Other than that, In the areas of banking and finance, data mining can be used to create risk models that are accurate when dealing with mortgages and loans. Fraudulent transactions can be detected through the use of mining, as well. (Insights, T.D., 2018).

On the other hand, it can be devastated if the company is not secure enough to protect the data they collected from the user. Hacker only need to target the company data bases to get all the privacy information about the users. Recent example is CIMB Bank Malaysia. CIMB stated that they had detected some suspicious external behavior towards its information and technology (IT) system. (Bernama, 2019). Luckily, they managed to resolve the problem within time. As you can see, mining data can benefit us as well as damage us.

Now let’s dive in on how to protect our privacy. To do that, we have to start from basic, our password. Yes, we have to protect our password. I’m not saying that you should create a complicated password, although it might work that way. Just create long enough password so that it takes time to be crack. This is because a complex password won’t prevent hacker using hacking tool to such as “oclHashcat” that make use the speed of Graphic processing units or GPUs to crack the password. (Mitnick, K.&Vamosi, R.,2017). So, when you create a 25 characters password, it will take time for the hacking tool to crack your password. But how do want to remember all this password? you don’t want to use the same password for two different account right. So, Its’ either you use the traditional way which is paper and pen or modern way which is software called password manager. Password manager act as a center base that will store all your valuable password. By using, this way you only have to remember password for your password manager only. If you feel it’s too complicated to a make a longer password and store it to password manager, it's okay as we have another approach to this problem. Let's say you want to create a password the old fashion way that you’ve choose some really strong password like your cat name Loki1Lico2 for your account bank. Of course, nobody will expect that but try to make it harder by cryptic it. Let’s say you, change the L to “!” and o to “0” instead, you password will be like this “!0ki1!ic02”. See it’s harder for someone to guess it.

Now you have secured your password, but do you think it will secure your data inside your laptop or smartphone? Well it not. Your data simply can be exploit by putting a malware inside your gadget. It then waiting for the right moment to your collect and then transfer to others person. You may say, you can use cloud services such as I Cloud, Google Drive or Microsoft One Drive to save your data. Trust me, it's is not guarantee safe as someone can intercept the data through networks by make sure all the data pass through his computer first before go to cloud services server. (Mitnick, K.&Vamosi, R.,2017). To prevent this from happening, you have to encrypt all your data first before you send to clouds server. There's a lot software that use end-to-end encryption out there that helps you to encrypt your data and one of them is GNU Privacy Guard. GnuPG allows you to encrypt and sign your data and communications, it features a versatile key management system, along with access modules for all kinds of public key directories. (GNU, 2015). The way this encryption work is that you will encrypt all your data with your private key, then only authorized receiver with correct public key can decrypt back the data to its original state. (Mitnick, K.&Vamosi, R.,2017). This way, hacker cannot read the data as they don't have the public key to decrypt it.

There's another one more precautious step that I think important too which is to clear all your cookies and history after you browse something especially when you use public services such as cybercafe where there will be a lot of people will use the same computer again and again. This is because some browser tends to save our password whenever we log in into certain website. But why the browser done that? By default, browser assume that you are the owner of this computer by saving the password so later on when you open the website again, you don't have to enter the password again. It has been manufactured that ways. However, most browser on the internet now have offer an alternative to browse anonymously. For example, incognito mode by Google Chrome. Other than that, you have to be extra careful when using auto backup or auto sync setting as you don't want others to see your sensitive information. Try to turn of the setting whenever you use public service or even better don't turn the setting on and do it manually. You also don't want to simply connect your device with unsecure Wi-Fi especially in "hot area" such coffee shop or library as it might be a network set up by hacker to collect your data. It's better to ask for confirmation from the shop first before you connect to it.

Lastly, I think the solution provided are pointless if you fail to secure your gadget in real life. What I mean by that is you let other people take control over your laptop when you not around. You see, it's kind of waste of time that you have create long and complicated password, encrypt all the data to know that it's easily being breach like that. So, you going to make sure that you bring all your gadget along with you and if the situation doesn't allow that for example, your computer. It's true you cannot carry your computer around as it is not practical to do so. You can put your computer to sleep mode or even better to set a timer so that it will automatically sleep by itself. Computer will lock automatically when it's enters sleep mode and prevent other from browsing inside your device. Apart from that, you also want to be careful with social engineering. Social engineering is the art of getting users to compromise information systems. Instead of technical attacks on systems, social engineers target human with access to information manipulating them into divulging confidential information. (Krombholz, K., Hobel, H., Huber, M., Weippl, E.,2015). Spear phishing are one of the ways of social engineering. So, you going to make sure who's you talking to before giving any sensitive information to prevent from being one of the victim social engineering.

To conclude, we have to protect our privacy because it is our right to do so. Privacy is important as our health, the more you take care of it, the less you don't have to worry about. Apart from that, we have to learn some knowledge about cybersecurity in order for us to be wise when browse something. This can prevent ourselves being one of the victims of scam or hacking or social engineering although some professional in cyber security also sometimes times can be unlucky. But it's better to at least have some knowledge rather than know nothing at all.

References

Alhamzah, T. (2019, August 2). ‘My wife knows where the nude photos come from’. The New Straits Time, p.1. Retrieved from https://www.nst.com.my

Bernama. (2019, September 6). ‘CIMB’s core banking services customer’s data intact’. The new Straits Time, p.1. Retrieved from https://www.nst.com.my

Insights, T.D. (2018, October 16). The Benefits of Data Mining. Retrieved from https://www.thinkdatainsights.com

Krombholz, K., Hobel, H., Huber, M., Weippl, E. (2015) Advanced social engineering attacks. Journal of Information Security and Applications, 22, 133-122. http://dx.doi.org/10.1016/j.jisa.2014.09.005

Mitnick, K., & Vamosi, R. (2017). THE ART OF INVISIBILITY, New York: Little Brown and Company

Parent, W.A. (1983). A new definition of privacy for the law. Journal of LAW and PHILOSOPHY, 2(3), 305-338 https://doi.org/10.1007/BF00144949

The GNU Privacy Guard. (2015). Retrieved September 19, 2019 from https://gnupg.org