Bad Impacts of Technology During Covid19

1st Ashiqur Rahaman Ridoy
CSE
AIUB
Dhaka, Bangladesh
ridoyashik@icloud.com

***Abstract*—In this age of computer science everything is getting easier with the help of technology. Mostly in the pandemic situation such as: tsunami, heavy rain, and virus. But there are some problem which is rising because of technology. Not every time technology help us or sometimes we cannot us the technology in the correct way and that's why we face different problem. The problems can be happen with the body or it can be raise problem for individual's personal information. So, in pandemic situation people don't do work that much and stay lazy most of the time and that's why they get sick. And sometimes they user their mobile phone or computer whole time and which effect their eyes very badly. And another thing is, as people are having lazy time and pass their most of the time on computer or mobile phone, it is the important time for hackers to do phishing attacks or Social Engineering.**

***Index Terms*—hacker, intruder, OSINT, Social engineering, phishing, social network**

I. Introduction

Technology is getting updated day by day and we cannot think about a moment without technology. People should more aware of their private information on the internet. Because, if a person use a social network app, then he/she may share his/her information every day. Sometimes they are so much addict to using their social network and they forget that what they are sharing. If just imagine, if an intruder want to harm a person then he don't need to do a lot research on the victim because the victim had already share everything on his social network. So, the intruder can easily analysis those data and can do whatever he want to do. So, people should aware of what they are doing on social network and what information is publicly available about him.

II. What is Social Engineering?

Engebretson (2011) [1] defines social engineering as "one of the simplest methods to gather information about a target through the process of exploiting human weakness that is inherit to every organization." In the first step social Engineering attack, attacker try find out a person who will be easy to manipulate and then try to his manipulating skill to hack into that person's mind and gather information. Social engineering is known as a low-tech attack; the attack aims at manipulating victims to let out confidential information and is roaring in its attempt thanks to exploiting temperament vulnerabilities. Social engineering as a tactic deploys techniques to gain access to non-public and confidential information by exploiting flaws in human logic know as psychological feature biases [2].

III. What is OSINT?

OSINT means Open source intelligence, it means gathering information about a person of an organization which can be gather legally or publically available. OSINT is one the most favorite things for hackers. Cause they can get a lot of information about the victim by using OSINT. In hacking methodology there are 5 phases and among them Reconnaissance is the first phase. And experts says, you should use more time on this phase. Because, sometime by using OSINT only hackers can get credentials also.

IV. What is Phishing:

Phishing is one of the hacking method which is done by making fool or deceiving the victim. It this technique hackers spoof the URL or website link to redirect users to suspicious websites that appear legitimate. When victim visit that website and provide information and send it to server it actually goes to hacker and hacker can see all the data

Fig. 1. Phishing attack

Identify applicable funding agency here. If none, delete this.

V. How technology effect during covid19:

Social engineering, OSINT and Phishing is directly connected to a human. This kind of attack is human based attack. So, if an attacker cannot communicate with that person then he cannot manipulate that person and attacker will not be succeed. So, in this technique of hacking there must be interaction with victim. In pandemic situation, people are staying their home. And they are passing their most of the time on internet. So it is the key time for hackers to manipulate their victim. It means, in normal days people might be busy and they don't have that much time to communicate with new people or passing their time on the internet but in pandemic situation they have a lot of time and can be vulnerable. I did a survey about how long people use their mobile or pc and which browser they use and which social media they use. From that survey I got something interesting. I found that all of them use Facebook and YouTube. And most of them are using mobile and pc average 8 hours in a day during pandemic situation. But from these people only 9.1% like to use personal computer for 8 hours in normal situation and only 27.3% like to use mobile phone for 8 hours in normal situation. And another important thing is most of them like to use chrome browser. Here are some figure of that survey: [3]

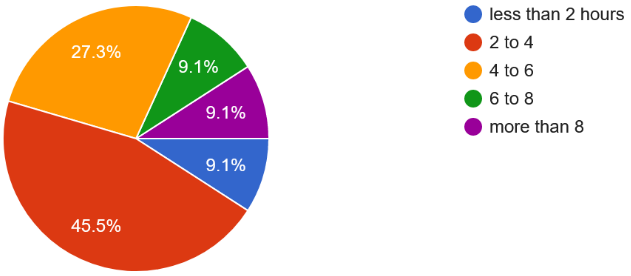

Fig. 2. Rate of using PC in normal situation

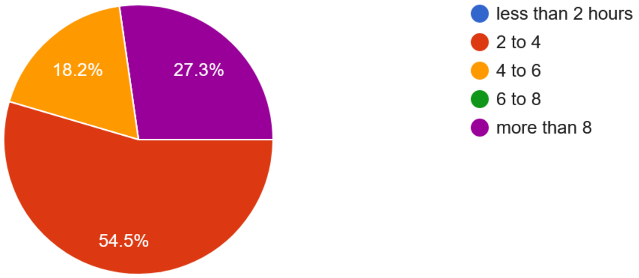

Fig. 3. Rate of using PC in normal situation

So, here if I want say how a hacker can hack into their system by using these data, first of all I will notice that what these people like to do most. As we can see they use Facebook and YouTube most so, in this situation I can do "man in the middle attack (MITM)" and "Address Resolution Protocol (ARP Poisoning)". In these attacks, MITM intersect the data flow between victim and server [4]. And then in ARP poisoning attack hacker will try to poison the "Domain Name System (DNS)" and change the Facebook address to a malicious address [5]. When victim visit that malicious address and provide information to that malicious website, it will go to hacker's database directly.

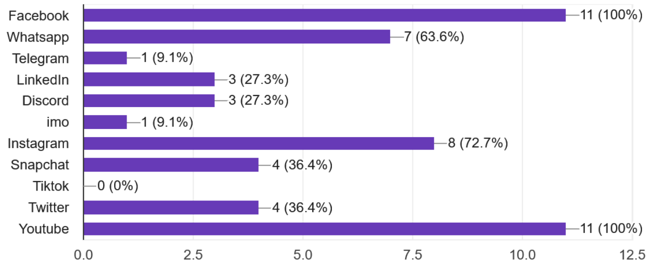

Fig. 4. Which app people use most

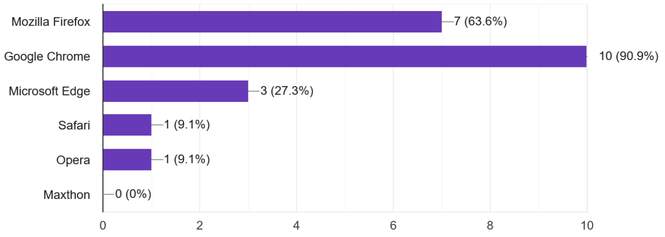

Fig. 5. Which browsers people use most

VI. Conclusion :

we need Technology everyday but we have to be safe and save our privacy from others. To do this we should be more aware of what we are doing and saying. Even sometimes filling up a survey from random person may harm you a lot. At the end I just want to say don't share your information.tep where is putting. In this situation to prevent this problem defense in depth structure should be stricter. To do so, organization can include a mixture of the precautionary measures:

References

[1] Engebretson P. The basics of hacking and penetration testing: ethical hacking and penetration testing made easy. Elsevier; 2011.

[2] Luo X, Brody R, Seazzu A, Burd S. Social engineering: the neglected human factor for information security management. Information Resources Management Journal. 2011; 24(3):1-8.

[3] A.R.Ridoy (14 Dec, 2020), Rate of Technology Uses, Retrieved from https://forms.gle/7hCeLcKhqzT9WXnh6

[4] Q. A. Chen, E. Osterweil, M. Thomas and Z. M. Mao, "MitM Attack by Name Collision: Cause Analysis and Vulnerability Assessment in the New gTLD Era," 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2016, pp. 675-690, doi: 10.1109/SP.2016.46.

[5] S. Kumar and S. Tapaswi, "A centralized detection and prevention technique against ARP poisoning," Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Kuala Lumpur, 2012, pp. 259-264, doi: 10.1109/CyberSec.2012.6246087.