

Manipulators on Internet in A Cyber Era

– Aamna Shahab

Bachelor of Computer Applications (BCA) 6th Semester, Amity University Noida, India

[@lamaamna](#) <https://orcid.org/0000-0001-7861-6014> aamna.shahab10@gmail.com

Article History

- Paper Nomenclature:** Scrutiny Tip (ST)
- Paper Code:** CYBNMV1N7DEC2019ST1
- Submission Online:** 02-Dec-2019
- Manuscript Acknowledged:** 11-Dec-2019
- Originality Check:** 13-Dec-2019
- Originality Test Ratio:** 2%
- Peer Reviewers Comment:** 15-Dec-2019
- Blind Reviewers Remarks:** 20-Dec-2019
- Author Revert:** 21-Dec-2019
- Camera-Ready-Copy:** 23-Dec-2019
- Editorial Board Citation:** 24-Dec-2019
- Published Online First:** 11-Feb-2020

In the era of technology at its evolving stage. We realize that the more the technology is evolving, the more the cybersecurity needs to be taken care of. When we talk about crime, it's mainly about murder, theft or any other criminal activity. Though, when we talk about Cybercrime, then things are taken to a different perspective. Cybercrime or as we can say, any computer-oriented crime takes place in the presence of a computer and a network. Any attacker will be using a computer to make the cyber attack feasible and a computer, on the other hand, will be there, ready to be attacked due to its low security. In other words, it can be said both the target and the weapon is a computer.

The most common cybercrime is the DDoS attack (Distributed DoS), it shuts down the system and networks using the system's own protocol against it.

Keywords : Cyber-attacks | Crypto-currency | Cyber Crime | Network | Data

Introduction

How do attackers attack?

This question is asked by several people who don't have any idea at what cost they are giving out their network information and to whom in just a click of "Yes, I agree to the terms and conditions" How their simple I.P Address and MAC address is being used in a way they cannot imagine.



This Photo by Unknown Author is licensed under CC BY-SA-NC
Fig. 1.

- Where there are confidential/ personal data, an opportunity and most importantly, an intention to do cybercrime. Thus, Data breach occurs which means that intentionally or unintentionally

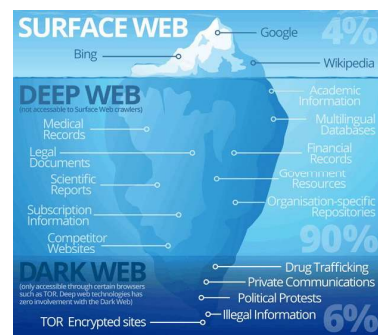
the release of secure or private/ confidential information to an untrusted environment can take place. It is the same as data leak, information leakage and also data spill. When a cybercriminal successfully infiltrates a **data** source and extracts confidential information. Either done physically by accessing a computer or network to steal local files or by bypassing network **security** remotely.



This Photo by Unknown Author is licensed under CC BY-SA-NC
Fig. 2.

- Whether it is the dark-web for selling things which are illegal

on whitelisted websites. Be it code, arms and ammunition and what not. Also, if our information is present on dark web, it can be used by criminals to commit fraudulent activity.



This Photo by Unknown Author is licensed under CC BY
Fig. 3.

- Even cryptocurrency is used for major cybercrimes, giving spam emails to people who are innocent. For example, A friend of mine was mailed that his video will

be uploaded on a pornographic website if he doesn't give a 100\$ to the account in bitcoins. So, there are many spammers who go to any level to make crime and try their best to not get caught. Though, many of them get caught and punished according to the law.



This Photo by Unknown Author is licensed under CC BY-SA Fig. 4.

- SMS like “You won 10000\$, Click below to Claim Now!” is definitely spam, You are really innocent and unaware of the consequences of clicking such links. I will let you know later in this article about the consequences.

Spams like backscatter spams occur when a humongous amount of e-mail messages gets bounced by the system.



“Wow! I’ve got one from someone I know!”

This Photo by Unknown Author is licensed under CC BY-NC Fig. 5.

- Phishing attacks are very common these days, they are the easiest way of attacking one’s bank account directly because the user himself/herself gives out the information for authentication of their original account. For Example: Rather than going to my ici.com website for net-banking purposes, someone accidentally clicked on a link which said, icic.com (one ‘i’ missing) as the user puts in all the information, the database of the attacker gets updated with the information of the

poor user who authenticated to a malicious website unknowingly. Then, the attacker goes to the original website and uses the USER ID and PASSWORD for monetary benefits.



This Photo by Unknown Author is licensed under CC BY-SA Fig. 6.

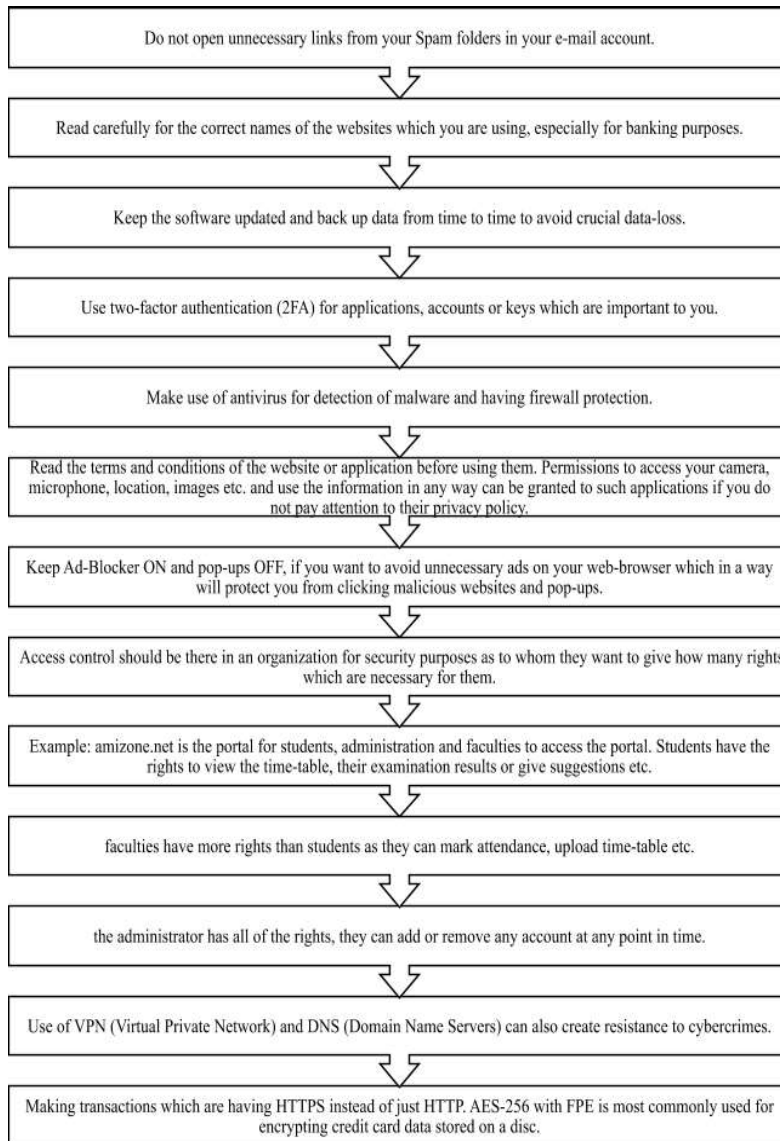
How to save ourselves from these attackers?

There are some tips which will help you to keep your device secure. Even though, there isn't a single antivirus available on this planet which would give you 100% security guarantee.

To save oneself from crimes, one should have a broad idea about the **types of cybercrimes**.

- CYBEREXTORTION:** A threat of attack which demands money to stop the attack. For example, Ransomware attack (attacker attacks the important files of an organization and encrypts them, thus files become inaccessible until a ransom is paid usually by using cryptocurrency like bitcoin).
- CYBERESPIONAGE:** When an attack is made for the purpose of gaining confidential information held by the government or any other huge organization.
- IDENTITY-THEFT:** When the attacker pretends to be the user and takes his identity for malicious purpose. For example, Health-related information of an individual, Audio/Video accounts etc.
- CREDIT-CARD FRAUD:** When an attacker gets into the system of an individual for the purpose of filtering credit-card information to sell the account information on the dark web.
- SOFTWARE PIRACY:** Unlawfully copying and distributing a software program for business/commercial purposes.
- CRYPTOJACKING:** Cryptocurrency mining software is loaded into the victim's system.
- EXIT SCAM:** Dark web has made it easier for criminals to even steal from other criminals while diverting virtual currency of other escrow accounts to their own accounts.

Ways to Protect Our Network:



This Photo by Unknown Author is licensed under CC BY-NC Fig. 7.

Conclusion and Future Scope

The chances after protecting your device are always less as to the one who is unaware of everything. Some people do not even know about their own system so it is always a good thing to know what system you are using, what are the various updates which can be done, which antivirus will protect your device best etc. All these decisions are beneficial as one should never compromise with their data. It is our data and we should always be an aware individual. We should know about where the data is shown, what is being done with it and to what extent it can be dangerous if someone have your information. Hence, as everything is available on the internet nowadays, it is impossible for anyone who has access to the internet, say, that they do not know about the cybercrimes. It is researched that in every 34 seconds, there is a cyberattack.

We have a sense that the attackers are always a step ahead but what we have to do as defenders is to make the attackers job harder and harder. Reputed institutes and universities are having courses for cybersecurity so that students are aware about the crimes and how they can handle them. The Internet of Things (IoT), driverless cars and all manner of different systems just show us that the need of IT security will definitely increase over time. It has boomed in the past 6-10 years and will continue to do so.

References

- <https://chiefexecutive.net/understanding-seven-types-data-breach>
- <https://www.pinterest.com/pin/51228514498646946>
- <https://managedmethods.com/blog/what-is-a-data-breach>
- <https://www.ajura.com/blog/data-breach-cyber-attacks-2018>



Aamna Shahab is a student of Amity University, pursuing her bachelors in computer applications (B.C.A). She has always been inquisitive about technology and programming. She has made android applications for food delivery services, weather services etc. with her team of developers. She has written a chapter with her mentor Dr. Neetu Mittal, titled “A Novel IoT Access Architecture Energy Efficient Solar Battery Charging System For Mobile Phones” for the Taylor & Francis Group, Scopus indexed giving her a cutting edge towards her chapter publishing road. She also has a patent concerning solar charging and wireless power transmission. She looks forward to innovating, research and develop something so powerful and useful for people to make lives easier.

[@lamaamna](#) aamna.shahab10@gmail.com

Annexure I

Submission Date	Submission Id	Word Count	Character Count
13-Dec-2019	D62558190 (urkund)	2353	11396



Urkund Analysis Result

Analysed Document: CYBER_Article_Aamna (1).docx (D62558190)
Submitted: 13/12/2019 3:57:00 PM
Submitted By: skesharwani@ignou.ac.in
Significance: 2 %

Sources included in the report:

<https://managedmethods.com/blog/what-is-a-data-breach/>
<https://www.ajura.com/blog/data-breach-cyber-attacks-2018/>

Instances where selected sources appear: 2

Note: Cybernomics runs an Urkund plagiarism tool for the originality check of an article before publication. Urkund is developed by Prio Infocenter AB based in Stockholm, Sweden.

Reviewers Comment

Review 1: This article contains all the latest facts and point which contains all the facts based in current scenario of cyber attack.

Review 2: In my opinion, if you are seeing investing in crypto currencies, it may be best to extravagance your “speculation” in the same way you would luxury any other highly hypothetical undertaking.

Review 3: The appearance of Bitcoin has flashed a argument about its future and that of other cryptocurrencies. Despite Bitcoin’s recent issues, its success since its 2009-10 launch has inspired the making of alternative crypto currencies like Litecoin,.

Editorial Excerpt

The article is satisfiable for publication after plagiarism check by our team on URKUND it has minor 2% plagiarism. The finding related to this particular manuscript seems to be noteworthy and defend a topic “**Manipulators on Internet in A Cyber Era**” Cyber security poses larger threat than any other spectrum of technology. Cyber criminals have already started abusing technology controlled devices for propelling cyber-crimes such as frauds and thefts. Hence is has been earmarked and decided under “**Scrutiny Tip (ST)**” category.

Acknowledgement

My special thanks to my parents (Mrs. Hera Shahab & Mr. Ansar Shahab) and all my faculty mentors who have always supported me, in my interests. I’m thankful to Dr. Himanshu Gupta who taught me concepts of cyber security with great examples. Special thanks to Ms. Rajbala Simon for motivating and giving me an opportunity to write the article “Manipulators on Internet in a Cyber Era” for Cybernomics.

Disclaimer

All Views expressed in this paper are my own, which some of the content are taken from open source website for the knowledge purpose. Those some of i had mentioned above in references section.

Citation

Aamna Shahab
 “Manipulators on Internet in A Cyber Era”
 Volume-1, Issue-7, Dec 2019. (www.cybernomics.in)

Frequency: Monthly, Published: 2019
 Conflict of Interest: Author of a Paper had no conflict neither financially nor academically.



Scholastic Seed Inc.
www.scholasticseed.in