0.7% PlagScan by Turnitin Results of plagiarism analysis from 2023-08-16 06:15 UTC

0457_02_IN710_0006_DHIVYESH_NOVEMBER 2023.docx

Date: 2023-08-16 06:14 UTC

✱ All sources **2** | Plagiarism Prevention Pool **2**

☑	[0]	from a PlagScan document dated 2021-03-11 11:50 **0.3%** 1 matches
☑	[1]	from a PlagScan document dated 2021-01-08 11:19 **0.3%** 1 matches

8 pages, 1891 words

PlagLevel: 0.7% selected / 0.7% overall

2 matches from 2 sources, of which 0 are online sources.

Settings

Data policy: *Compare with web sources, Check against my documents, Check against my documents in the organization repository, Check against organization repository, Check against the Plagiarism Prevention Pool*

Sensitivity: *Medium*

Bibliography: *Consider text*

Citation detection: *Reduce PlagLevel*

Whitelist: --

Individual Research Report

Candidate Name: Dhivvyesh Kumar

Candidate Number:0006

School Name: Arsha Vidya Mandir

School code: IN710

Component code: 02

Topic: Digital World

Word Count: 1905

Question: Why do hackers steal people's personal information? How might this risk be diminished?

Why did I choose this topic?

I chose this topic because people are getting hacked often which leads to a major money, digital data and physical equipment too. When I read an article from The New Indian Express published:216th June 2022, which said that business account of 5-star hotel named Crown plaza which is located in Kochi, Kerala got hacked which lead to a major loss of money and digital data. So I was curious to know about the countries which have a high rate of hackers and the reasons behind hacking.

Introduction:

In order to steal, alter, or erase information, hackers typically break into internet-connected devices like computers, tablets, and smartphones.

To make money on the dark web, hackers sell your personal information to other criminals. The data is used by criminals to commit crimes. Users of a lot of online services are required to enter personal information such their complete name, home address, and credit card number. Criminals steal this information through internet accounts, such as the victim's credit card or loans taken out in the victim's name.

thieves take jewellery, cash, etc., but hackers take digital information like bank passwords and identification. By installing malware—malicious software used for hacking—such as worms, trojan horses, spyware, etc.—they not only take data but also wipe it. These programmes take control of your device without your knowledge.[1].

Types of hacking

1) Financial hackers-hackers make fake transactions and gain account information, credit card numbers which results in loss of money.

2) Hacktivism- Hacktivism is a form of vandalism; it is the use of computer-based techniques such as hacking.

3) Legal hacking-Also known as White hat hacking. It is used to identify security vulnerabilities in hardware, software or in network[2].

Types of hackers:

1) Black hat hackers-

[1] http://www.ijcst journal.org/volume-2/issue-6/IJCST-V2I6P2.pdf

[2] http://www.ijcst journal.org/volume-2/issue-6/IJCST-V2I6P2.pdf

Black hat hackers are the ones who take part in cybercrime and use hacking for income. Thirty years ago a black hat hacker, Kevin Mithinick, was the FBI most wanted cybercriminal for hacking high tech companies like Nokia.

2) White hat hackers-

White hat hackers are known as ethical hackers because they use their hacking skills to find security vulnerabilities in a system, hardware and network.

3) Grey hat hackers-

Grey hat hackers are a mix of white hat and black hat hackers because they look for vulnerabilities in a system without the owner's permission and report it to the owner demanding a fee[3].

Impact of Hacking

Enterprises (both huge firms and tiny start-up businesses) are one of the main targets of hacking. They suffer a great loss since they are frequently targeted by their own staff (depends upon the company). Because the network has already been compromised and other businesses are concerned that their data would leak, they will consider investing in the hacked firm and spending a lot of money to restore the network.

Hackers and Medical Industries

From the IT sector to the medical sector, hackers are not abandoning any businesses. Assuming that a hospital's network has been compromised, there would be a lot of issues because the medical sector is currently quite profitable, therefore if the account were compromised, the hospital would suffer a significant loss. In Chennai, the average cost of an ICU stay is about 8,000 per day, and during the pandemic situation, many individuals were admitted to hospitals (cost of per day during pandemic situation is 20000 to 25000). Assume the hospital will lose everything if the account is compromised.

[3] https://www.researchgate.net/publication/316431977_Ethical_Hacking_and_Hacking_Attacks

Global perspective:

Top 4 countries with the most hackers

1) China

2) United States

3) Turkey

4) Russia

China

- China has around 48.3 million companies (including MNC).
- China has a cyber-warfare unit.
- The NSA (National Security Agency) has conducted more than 10,000 vicious cyber-attacks on China.
- China loses $66.3 billion every year due to hacking[4].

USA .

- There are 481,240 businesses in USA as of 2022, increase of 2.2 percent compared to 2021
- WannnaCry ransom ware attack-WannaCry ransom ware is malicious software that blocks user access to files and system. To access the files the victim should pay money in exchange to access the files and system.
- This attack harmed computers across 150 countries
- This incident began at 07:44 a.m. on 12th May 2017 few hours later this incident came to an end at 15:03 p.m.
- The United States and the United Kingdom formally arrested North Korea as they were behind this.
- The United States loses $19.4 billion every year due to hacking[5].

Turkey

- Turkey has over 6000 global companies
- One of biggest cyber-attack in Turkey was when APT groups of company

[4] https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1413&context=etd

[5] https://sbgsmedia.in/2018/05/10/2261f190e292ad93d6887198d7050dec.pdf

detected 42,136 phishing attacks targeting millions of people. It was detected by SOC radar (it's a tool to monitor potential risks)[6].

Russia

- Russia has over 529,300 business.
- Russia has skilled hackers that they even hacked Ukraine power grid. It resulted in power outages for over 230,000 consumers for 1-6 hours.
- The Ukraine government says that they have used a new variant of malware called "Industroyer". Industroyer is a malware used to hack electrical grids. It is designed to disrupt the process of control system[7].

National perspective:

In India .the government is unable to control cyber-attacks. The two main reasons behind the high rate of hacking is lack of defensive cyber security and the other reason is that the cyber security projects in India is lesser in number compared to other countries. The Indian Government has told that the hackers have increased mainly in the banking and financial sectors. India is racked 85 th in internet connectivity but it is ranked 7th in terms of cyber-attacks. In 2013 alone, India saw an increase of 136 percent in terms of cyber-attacks and attacks against the government has increased by 126 percent. Around 69 percent of cyber-attacks have targeted large companies.

The IT (Information Technology) sector in India is the main reason for the economic growth of India as well as hackers. For instance, after India's nuclear test in May 1998, hackers started to post anti-India and anti-nuclear messages on Bhabha Atomic Research Centre's (BARC) website. They didn't stop it with posting messages; they also leaked some sensitive data of the research centre. Another major cyber-attack is when hackers hacked the automatic power grid in north India this resulted in blackout. This affected 670 million peoples life not only that, it also affected the services of north India like the railways and road traffic signals[8].

Haryana:

Officials said that till august of 2022 there was 36,996 cases were received in the helpline number (1930).Over 20,000 of cases are unsolved. Panipat and Sonipat was the top 2 district with the most complaints[9].

[6] https://www.reuters.com/article/us-cyber-attack-hijack-exclusive-idUSKBN1ZQ10X

[7] https://www.wsj.com/articles/google-sees-russia-coordinating-with-hackers-in-cyberattacks-tied-to-ukraine-war-11663930801

[8] https://www.academicapress.com/journal/v1-1/Parmar_Cybersecurity-in-India.pdf

Karnataka:

Karnataka has over 17, 48,000 companies. In the last 3 years Karnataka lost over 220 crores to cyber-attacks and has recovered about 21 percent of the money which is 47 crores.

Maharashtra:

Maharashtra's power grid was once hacked by Chinese hackers. This attack began at 10a.m on October 12, 2022. Because of this attack the connection with Mumbai through railway was disconnected.[0] This attack led to huge loss to companies as it is the financial capital of India and the whole stock market was down because Bombay Stock Exchange and National stock exchange is located here[10].

The Indian Government has taken various actions like ‘the Indian Computer Emergency Response Team (CERT-In). It works as a national agency to get a grip of the country's cyber-attack on government networks. More actions like this are going to be implemented to make India have a safer internet[11].

Personal perspective:

According to me, hackers can change the coding in the server which causes the database to shut down or they can steal the valuable information, username and password, credit card number etc. To protect from this we can keep our server's location a secret or we can use strong firewalls such as Cisco firepower, Netgear proSAFE, MacAfee etc .Firewall is something which is used to secure the database and to prevent unauthorised entries.

If we need to reduce the rate of hackers in countries and to reduce the loss due to hacking we need to be united but that won't happen if the government itself hack other countries. In September 2014 few Chinese hackers hacked databases belonging to U.S.A such as U.S airlines, U.S based companies, U.[1]S military equipment etc with the support of the Chinese government.

Some countries have many skilled hackers who can hack big databases with high security. One such country is North Korea .North Korea is so poor that 60 percent of its population is under the poverty line and 24 million of them are facing extreme

[9] https://www.business-standard.com/article/current-affairs/haryana-reports-37-000-cybercrime-cases-till-august-15-000-disposed-of-122091600217_1.html

[10] https://www.indiatoday.in/india-today-insight/story/chinese-cyber-attack-why-maharashtra-should-worry-1774905-2021-03-02-

[11] https://www.academicapress.com/journal/v1-1/Parmar_Cybersecurity-in-India.pdf

poverty. The poverty per capita is $1,800(which is 2 percent of South Korea's GDP per capita) yet the country is so good at hacking that they hacked the Sony pictures and the other incident is that they installed a malware in a video game used by the South Koreans and they got control over 20,000 cell phones[12].

Possible scenario:

If we don't take actions on hackers, they will continue hacking which will lead many problems like:

1. Hackers will hack databases and steal sensitive information like card details etc. This will cause identity fraud[13].
2. Hackers would target Banks, business because they can gain more money when hacking in these sectors by making unauthorized attacks and financial fraud[14]
3. Hacker would target power grid and transportation sector because these will cause a long-time problem[15].
4. Hackers would hack healthcare systems, medical devices putting patients' life at risk and this can lead to breaches of medical information.
5. When a country attacks other country's government database they get access to their sensitive information and military network. This would create a cyber-war between nations.

Possible Course of action:

To keep your database safe from hackers you can use firewalls, Anti-virus software, and ignore links from strangers.

Firewall is a device which monitors the entries to the database and decides whether to accept it or to block the entry. It prevents communication with sources you don't permit. One of the most famous firewalls is MacAfee firewall.

Since new viruses are constantly being introduced into computers by hackers, antivirus software starts by scanning the papers, files, and apps on your computer. It will also check a machine or database for malware risks.

You should disregard links sent to you by strangers since they may be phishing links. There have been numerous occurrences similar to this one, in which consumers

[12] https://www.vox.com/2014/12/18/7413229/north-korea-hack-sony

[13] https://www.techtarget.com/whatis/feature/How-do-cybercriminals-steal-credit-card-information

[14] https://www.knowledgehut.com/blog/security/cyber-security-in-banking

[15] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8473297/

received anonymous links from hackers promising them 50GB of data, but as soon as they clicked the link, their device was compromised.[16].

Conclusion:

In addition to these countries, other countries are also experiencing hacking, with many victims suffering financial losses. Technology must be used constructively; destructive use is not acceptable. Hackers must cease hacking and apply their expertise for the benefit of the nation's economy. Some countries even provide government assistance to hackers. To stop this, worldwide cooperation and a better understanding of cyber security would be required.

[16] https://www.businessnewsdaily.com/11213-secure-computer-from-hackers.html