IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10443

Cybercrime: Security Threats and Solutions

J. Mohamed Kasim

Department of Electronics and Communication Engineering,

Annamalai University, Chidambaram, Tamil Nadu, India.

Abstract: Cyber related crimes are increasing enormously across the world. Hacking and viruses are used to steal important personal information. Understanding cybercrime is essential to understand how criminals are using the internet to commit various crimes and what can be done to prevent these crimes from happening. The Internet is a place saturated with information and over the years, information has become more easily accessible than ever before. How much information that is chosen to be shared on the internet should be carefully considered. A simple post to any social media site could give out more personal information than originally intended. Cyber security is a priority with the growing use and ease of access of the internet. If an internet user is not careful about the information given over to cyberspace, the user's identity could easily be stolen or their finances drained. Cyber security is important not just to the government but also to the average user. The field is of growing importance due to the increasing reliance on computer systems in most societies. Computer systems now include a very wide variety of "smart" devices, including smartphones, televisions and tiny devices as part of the Internet of Things (IoT) and networks include not only the internet and private data networks, but also Bluetooth, Wi-Fi and other wireless networks. Cybercriminals are attacking the computer networks and systems of individuals, businesses and even global organizations at a time when cyber defences might be lowered due to the shift of focus to the COVID-19 health crisis. This paper will cover different kind of cybercrimes, statistics on cybercrime, cyberattacks, COVID-19 impact on cybercrimes and information on what the average internet user can do to protect themselves from falling victim to cybercrimes.

Keywords: Cybercrimes, Cyber Security, Cyberattacks, COVID-19 impact on cybercrimes.

I. INTRODUCTION

The Cybercrime also called as Computer crime, is any crime that involves a computer and a network. As individuals and businesses increase their reliance on technology, they are exposed to the growing cybercrime threats. Using the computers for our day-to-day transactions is quite common now a days. For example, we pay our life insurance premium, electricity bills, reserve flight or train or bus tickets, order book or any other product online using personal computer, smart phones, public browsing centers etc. The number of users doing online transactions are growing rapidly ever since, because of the convenience it gives to the user to transact business without being physically present in the area where the transaction happens. Criminals committing cybercrime are also growing day-by-day with the increased number of users doing online transactions. Cybercrime covers a wide range of different attacks such as cyber extortion, cyber warfare, spreading computer viruses or malware, internet fraud, spamming, phishing, carding (fraud), child pornography and intellectual property rights violation etc. Because of increased cyberattacks these days, the internet users must be aware of this kind of attacks and need to cautions while doing online transactions and while browsing the internet.

II. CYBERCRIME

A generalized definition of cybercrime may be **"unlawful acts wherein the computer is either a tool or target or both".** Cybercrime is a crime in which a computer or the internet is used for a crime like hacking, spamming, phishing & etc. These kind of acts are punishable by "information technology act 2000". Information technology act 2000 is an act of Indian parliament notified on 17 October 2000. It is the primary law in India dealing with cybercrime such as to provide legal recognitions for electronic communications, data interchange & etc.

III. CLASSIFICATIONS OF CYBERCRIME

The Subject of Cybercrime may be broadly classified under the following three groups.

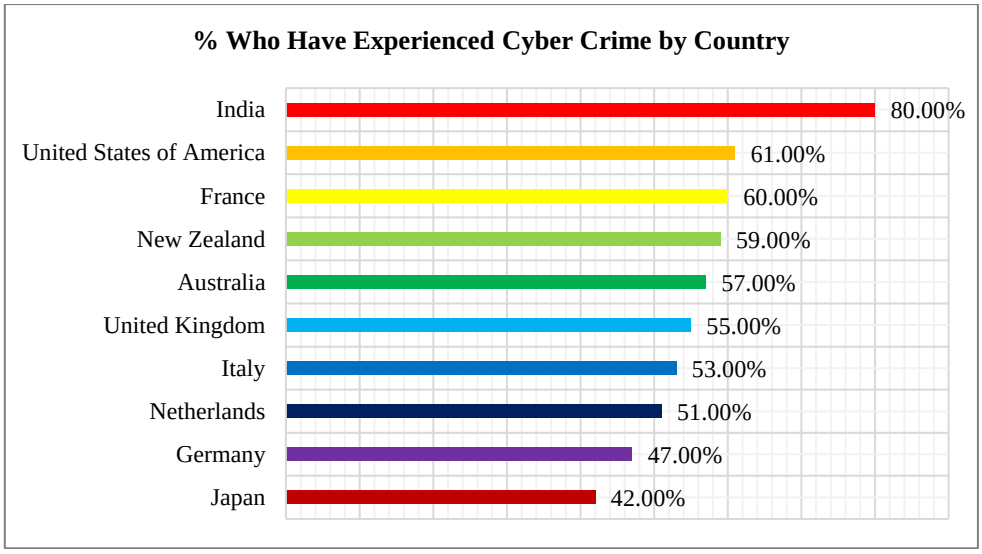
1. **Against Individuals**:
- Defamation of a person or their property,
- Unauthorized control or access over computer system,
- Transmitting virus,

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 10, Issue 4, April 2021
DOI 10.17148/IJARCCE.2021.10443

- Cheating & Fraud via email spoofing,
- Computer vandalism,
- Internet time thefts.

2. Against an Organization:
- Unauthorized control or access over the computer systems of an organization,
- Possession of unauthorized information,
- Distribution of pirated software,
- Industrial spying,
- Cyber Terrorism against the government organization & other various organizations.

3. Against the Society at Large:
- Pornography (Basically child pornography),
- Online gambling,
- Trafficking,
- Financial crimes & forgery,
- Polluting the youth through indecent exposure,
- Sale of illegal articles.



Based on 2019 NortonLifeLock Cyber Safety Insights Report

IV. MAJOR KINDS OF CYBERCRIME

There are various types of cybercrimes present in the internet. Some of the important cybercrimes are:

1. Social engineering:
It is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software that will give them access to your passwords and bank information as well as giving them control over your computer. Criminals use this tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password.

2. Phishing:
It is a process of acquiring personal and sensitive information of an individual via email by disguising as a trustworthy entity in an electronic communication. The purpose of phishing is identity theft and the personal information like username, password, and credit card number etc. may be used to steal money from user account. If a telephone is used as a medium for identity theft, it is known as Vishing (voice phishing). Another form of phishing is Smishing, in which SMS is used to lure customers.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10443

3. Cyber Stalking:
It is an act of stalking, harassing or threatening someone using internet and computer as a medium. This is often done to defame a person and use email, social network, instant messenger, web-posting and etc.

4. Child Pornography:
It is an act of possessing image or video of a minor (under 18) and engaged in sexual conduct.

5. Forgery and Counterfeiting:
It is a use of computer to forgery and counterfeiting is a document. With the advancement in the hardware and the software, it is possible to produce counterfeit which matches the original document to such an extent that it is not possible to judge the authenticity of the document without expert judgement.

6. Software Piracy:
Software piracy is an illegal reproduction and distribution for personal use or business. It comes under crime related to IPR infringement. Some of the other crimes under IPR infringement are downloading pirated movies, music, books and etc.

7. Computer Vandalism:
Damaging or Destroying data rather than stealing by transmitting virus.

8. Computer Hacking:
The Gaining of unauthorized access to data in a system or computer. The purpose of hacking a computer system may vary from simply demonstrations of the technical ability, to sealing, modifying or destroying information for social, economic or political reasons.

9. Spamming:
It is the act of sending unimportant bulk messages over internet. Spam emails are the computer version of unwanted "junk mail" that arrives in a mailbox, such as advertising pamphlets and brochures.

10. Cyber Squatting:
Act of reserving a website domain name of someone else trademark and later sell it to a very higher price to the organization who is the owner of trademark.

11. Web Jacking:
The hacker gain access to a website of an organization and either blocks it or modify it to serve political, economical or social interest.

12. Salami Attack:
It is a kind of small attack but when they are joined together it forms a major attack. For Example: Hacking a money of Rs 10 from 10,000 customers leads to Rs.1 Lakh amount of hacking.

13. Malvertising:
Malvertising means malicious online advertising.

14. Eaves dropping:
It is the Act of secretly listening to the private conversations of other's without their knowledge. It is an unauthorized real time interception of a private conversations.

15. Logic Bombs:
Malicious code which destroys data and information's on a system.

16. Denial of Service Attack (DoS):
It is a cyberattack in which the network is chocked and often collapsed by flooding it with useless traffic and thus preventing the legitimate network traffic.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10443

17. Distributed Denial of Service (DDoS) attacks:

Distributed Network Attacks are often referred to as Distributed Denial of Service (DDoS) attacks. This type of attack takes advantage of the specific capacity limits that apply to any network resources such as the infrastructure that enables a company's website. The DDoS attack will send multiple requests to the attacked web resource with the aim of exceeding the website's capacity to handle multiple requests and prevent the website from functioning correctly. Typical targets for DDoS attacks include Internet shopping sites and any business or organisation that depends on providing online services.

18. Man-in-the-middle attack:

A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecure Wi-Fi network, an attacker could intercept data being passed from the victim's device and the network.

19. SQL injection:

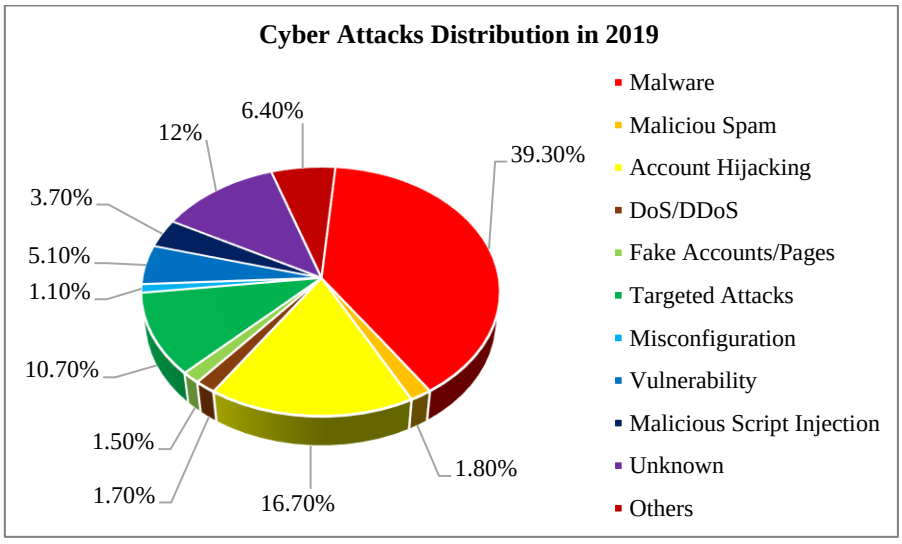
An SQL (Structured Query Language) injection is a type of cyberattack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a databased via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

20. Data Diddling:

It is a practice of changing the data before its entry into the computer system.

21. Email Spoofing:

It is a process of changing the header information of an e-mail so that its original source is not identified and it appears to an individual at the receiving end that the email has been originated from source other than the original source.



Based on 2019 Cyber Attacks Statistics report by Paolo Passeri (hackmageddon.com)

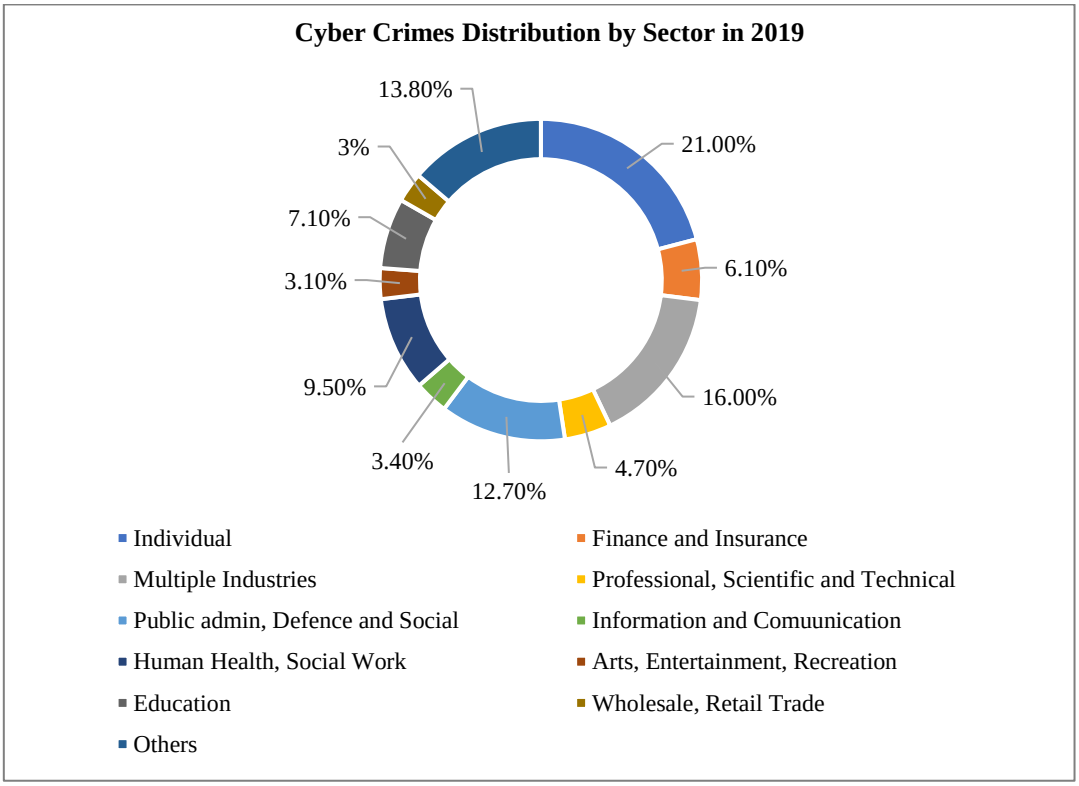
IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10443



Based on 2019 Cyber Attacks Statistics report by Paolo Passeri (hackmageddon.com)

V. MALWARE

Malware stands for "Malicious Software" and it is designed to gain access or installed into the computer without the consent of the user. They perform unwanted tasks in the host computer for the benefit of a third party. There is a full range of malwares which can seriously degrade the performance of the host machine. There is a full range of malwares which are simply written to distract/annoy the user, to the complex ones which captures the sensitive data from the host machine and send it to remote servers. 92% of malware is delivered by email. Mobile malware on the rise with the number of new malware variants for mobile increased by 54% in 2018. There are various types of malwares present in the internet. Some of the popular ones are:

1. Adware:
It is a special type of malware which is used for forced advertising.

2. Spyware:
It gathers the browsing habits of the user and the send it to the remote server without the knowledge of the owner of the computer.

3. Browser Hijacking Software:
This software modifies the browsers setting and redirect links to other unintentional sites.

4. Trojan Horse :
Trojan horse is a malicious code that is installed in the host machine by pretending to be useful software. Trojans make up 51.45% of all malware. The user clicks on the link or download the file which pretends to be a useful file or software from legitimate source. It not only damages the host computer by manipulating the data but also it creates a backdoor in the host computer so that it could be controlled by a remote computer. It can become a part of botnet(robot-network), a network of computers which are infected by malicious code and controlled by central controller.

5. Password Trojans:

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10443

These Trojans are designed to steal passwords and other types of information such as IP address, registration details, e-mail client details, and so on. This information is then sent to an e-mail address coded into the body of the trojan.

6. Ransomware:
It holds the host computer hostage until the ransom is paid. The malicious code can neither be uninstalled nor can the computer be used till the ransom is paid.

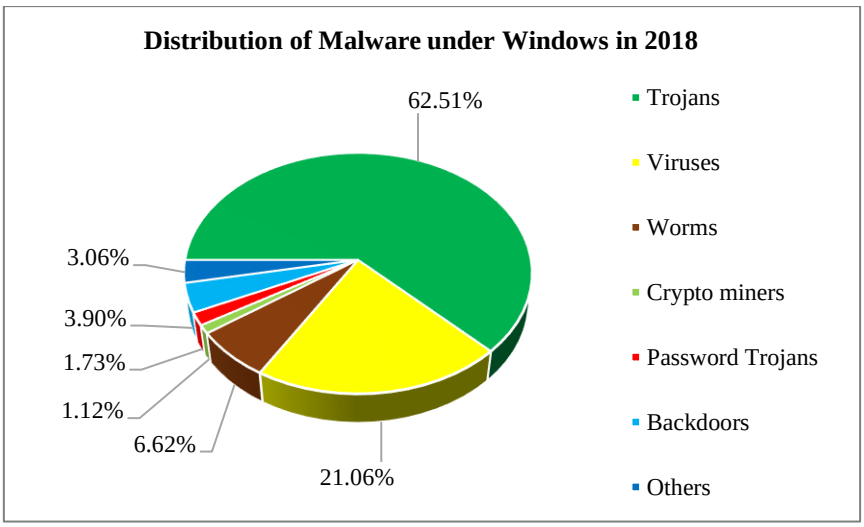
7. Botnets:
Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

8. Virus:
A virus is a malicious code written to damage/harm the host computer by deleting or appending a file, occupy memory space of the computer by replicating the copy of the code, slow down the performance of the computer, format the host machine, etc. It can be spread via email attachment, pen drives, digital images, e-greeting, audio or video clips, etc. A virus may be present in a computer but it cannot activate itself without the human intervention.

9. Worms:
They are a class of virus which can replicate themselves. They are different from the virus by the fact that they does not require human intervention to travel over the network and spread from the infected machine to the whole network. Worms can spread either through network, using the loopholes of the Operating System or via email.

10. Crypto jacking/Crypto Miners:
Crypto jacking is the unauthorized use of someone else's computer to mine cryptocurrency. Hackers do this by getting the victim to click on a malicious link in an email that loads crypto mining code on the computer, or by infecting a website with JavaScript code that executes once loaded in the victim's browser.

11. Backdoor:
A backdoor is a malware type that negates normal authentication procedures to access a system. As a result, remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware.



Based on the AV-TEST Security Report 2018/2019

VI. CYBERATTACK

A cyberattack is any attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage. Cyberattacks aim to disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal the data held within these systems. Stealing, modifying or even destroying the information without the user knowledge is the most common purpose for an attack which takes place on multiple organizations. The

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10443

average cost of a malware attack on a company is $2.4 million. 98% of cyberattacks rely on social engineering. A cyberattack can be launched from anywhere by any individual or group using one or more various attack strategies. Cyberattacks are classified as structured attacks and unstructured attacks.

i. Structured attacks:

Structured attacks are performed by highly skilled and experienced attackers with a clear motive. The structured attacks are mostly used by the criminals, terrorists and politicians for various reasons.

ii. Unstructured attacks:

Unstructured attacks are performed by immature attackers. They have no motive to perform cyberattack. These attackers are always use the software which is created by the advanced attackers. The unstructured attacks are mostly used by the beginning level hackers to gain access in to the system and to attack it.

VII. CYBERCRIMINAL

Cybercriminals are individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data, and generating profit. The major types of cyber criminals are:

A. Children and adolescents between the age group of 6 – 18 years:

The simple reason for this type of delinquent behaviour pattern in children is seen mostly due to the inquisitiveness to know and explore the things. Other cognate reason may be to prove themselves to be outstanding amongst other children in their group.

B. Organised hackers:

These kinds of cyber criminals are mostly organised together to fulfil certain objective. The reason may be to fulfil their political bias, fundamentalism, etc.

C. Professional hackers:

Their work is motivated by the colour of money. These kinds of hackers are mostly employed to hack the site of the rivals and get credible, reliable and valuable information. Further they are employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes.

D. Discontented employees:

This group include those people who have been either sacked by their employer or are dissatisfied with their employer. To avenge they normally hack the system of their employee.

VIII. HACKER AND THEIR MAJOR TYPES

A hacker is just a person who uses computer programming or technical skills to overcome a challenge or problem. Computer Hacking is a practice of stealing, modifying or destroying information for social, economic or political reasons. The hackers may be classified as:

1. White Hat Hacker: (THE GOOD GUYS)

They are legally paid Employee who is known as “Ethical Hackers”. Now the corporate are hiring hackers, a person who is engaged in hacking computers, to intentionally hack the computer of an organization to find and fix security vulnerabilities.

2. Black Hat Hacker: (THE BAD GUYS)

They are illegally paid hackers who are known as ‘Crackers’.

3. Grey Hat Hackers: (THE IN-THE-MIDDLE GUYS)

They Find Security Vulnerabilities & Report it to the sites such as Facebook, Instagram and others for consultancy Fees & they do not have any malicious intentions.

4. Blue Hat Hackers: (THE REVENGE GUYS)

They are typically new to hacking, they are motivated by any kind of personal revenge and do not think much of the consequences.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10443

5. Red hat hackers: (THE DO-WHAT-THEY-WANT GUY)
They are similar to policing agents on the internet. They actively search for black hat hackers and shut them down.

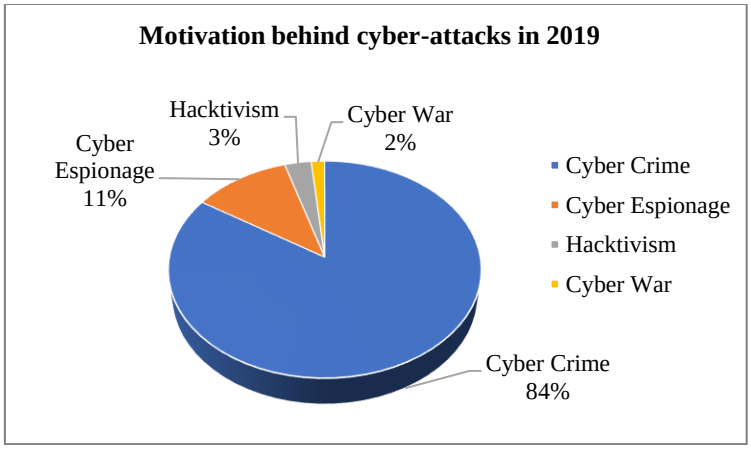
6. Green Hat Hackers: (THE BEGINNERS)
They are new ones & working to improve their skills every day so they can become better hacker.

IX. Reasons For Commission of Cybercrimes

There are many reasons which act as a catalyst in the growth of cybercrime. Some of the prominent reasons are:

i. **Money** - People are motivated towards committing cybercrime is to make quick and easy money.
ii. **Revenge** - Some people try to take revenge with other person, organization, society, caste or religion by defaming its reputation or bringing economical or physical loss. This comes under the category of cyber terrorism.
iii. **Fun** - The amateur do cybercrime for fun. They just want to test the latest tool they have encountered.
iv. **Recognition** - It is considered to be pride if someone hack the highly secured networks like defence sites or networks.
v. **Anonymity** - Many time the anonymity that a cyber space provide motivates the person to commit cybercrime as it is much easy to commit a cybercrime over the cyberspace and remain anonymous as compared to real world. It is much easier to get away with criminal activity in a cyber world than in the real world.

X. Motivations for Commission of Cyberattacks



Based on 2019 Cyber Attacks Statistics report by Paolo Passeri (hackmageddon.com)

1. Cybercrime:
It includes single attackers or groups targeting systems for financial gain or to cause disruption.

2. Cyber Espionage:
At times the government itself is involved in cyber trespassing to keep eye on other person, network and country. The reason could be politically, economically and socially motivated.

3. Cyber Warfare:
Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through transmitting computer viruses or denial-of-service (DoS) attacks. RAND research provides recommendations to military and civilian decisionmakers on methods of defending against the damaging effects of cyber warfare on a nation's digital infrastructure.

4. Cyber Terrorism:
It is defined as the use of computer resources to intimidate or coerce government, the civilian population or any segment thereof in furtherance of political or social objectives.

5. Hacktivism:
It is the act of misusing a computer system or network for a socially or politically motivated reason. Individuals who perform hacktivism are known as hacktivists.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10443

XI. COVID-19 CYBER THREATS

The pandemic of COVID-19 and the imposed lockdown, has led to more people to be confined at home with many more hours to spend online each day and increasingly relying on the internet to access services, they normally obtain offline. The dangers of cybercrime have been there for many years, but the increase in the percentage of the population connected to the internet and the time spent online, combined with the sense of confinement and the anxiety and fear generated from the lockdown, have provided more opportunities for cybercriminals to take advantage of the situation and make more money or create disruption. It is important to note that some more vulnerable segments of the population, such as children need to spend more time online for services such as schooling. This seismic change in how we live our lives and use the internet has prompted a proliferation of e-crimes. With organizations and businesses rapidly deploying remote systems and networks to support staff working from home, criminals are also taking advantage of increased security vulnerabilities to steal data, generate profits and cause disruption. Common cybercrime techniques, such as phishing and online scams have seen a spike. The Cyber Crimes that are increased enormously during the COVID-19 pandemic are:

1. Phishing & Online Scamming:
Threat actors have revised their usual online scams and phishing schemes. By deploying COVID-19 themed phishing emails, often impersonating government and health authorities, cybercriminals entice victims into providing their personal data and downloading malicious content. 1.5 million new phishing sites are created every month. In 2020 to date, 52% of phishing sites have used target brand names and identities in their website addresses. Based on F5 labs phishing and fraud report, phishing incidents rose 220% during the height of the global pandemic compared to the yearly average. Around two-thirds of member countries which responded to the global cybercrime survey reported a significant use of COVID-19 themes for phishing and online fraud since the outbreak.

2. Hacking at companies and offices:
According to a recent report by PricewaterhouseCoopers, the number of cyberattacks on various firms has increased manifold times since the corona outbreak. Companies have set up a VPN structure, to let the employees have access to all the information, which has become the target of the hackers. Hackers are trying to hack the software of the companies in order to gain access to all their important details and data. The use of an already-made malware 'AZORult' has increased for phishing into the companies. There have been cases of unwanted software trying to infiltrate to the companies' systems for theft and malicious payloads. Hackers have even attempted to hack the computers of the Indian State Tax Department to steal sensitive information of PAN Cards, GST numbers, phone numbers, and e-mails. There have been several attempts made by the hackers at banks and Stock Markets leading to the brokerage. Prime Minister of India's COVID fund has also been one of the targets of the Hackers.

3. Disruptive Malware (Ransomware and DDoS):
Cybercriminals are increasingly using disruptive malware against critical infrastructure and healthcare institutions, due to the potential for high impact and financial benefit. In the first two weeks of April 2020, there was a spike in ransomware attacks by multiple threat groups which had been relatively dormant for the past few months. Law enforcement investigations show the majority of attackers estimated quite accurately the maximum amount of ransom they could demand from targeted organizations.

4. Data Harvesting Malware:
The deployment of data harvesting malware such as Remote Access Trojan, info stealers, spyware and banking Trojans by cybercriminals is on the rise. Using COVID-19 related information as a lure, threat actors infiltrate systems to compromise networks, steal data, divert money and build botnets.

5. Malicious Domains:
Taking advantage of the increased demand for medical supplies and information on COVID-19, there has been a significant increase of cybercriminals registering domain names containing keywords, such as "coronavirus" or "COVID-19". These fraudulent websites underpin a wide variety of malicious activities including Command and Control [C&C] servers, malware deployment and phishing. From February to March 2020, a 569 per cent growth in malicious registrations, including malware and phishing and a 788 per cent growth in high-risk registrations were detected and reported to INTERPOL by a private sector partner.

6. Misinformation:
An increasing amount of misinformation and fake news is spreading rapidly among the public. Unverified information, inadequately understood threats, and conspiracy theories have contributed to anxiety in communities and in some cases facilitated the execution of cyberattacks. Nearly 30 per cent of countries which responded to the global cybercrime survey

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10443

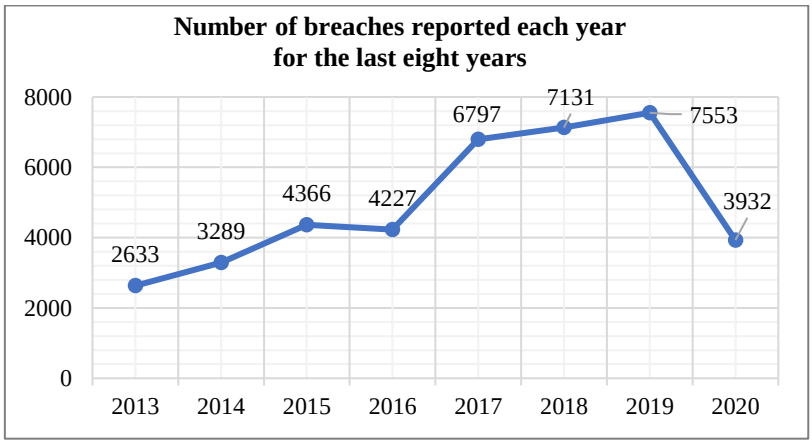
confirmed the circulation of false information related to COVID-19. Within a one-month period, one country reported 290 postings with the majority containing concealed malware. There are also reports of misinformation being linked to the illegal trade of fraudulent medical commodities. Other cases of misinformation involved scams via mobile text-messages containing 'too good to be true' offers such as free food, special benefits, or large discounts in supermarkets.

7. Patients at risk:
There have been cyberattacks not only at local hospitals or test centres but also at the World Health Organization (WHO) to steal the passwords of WHO workers. Ransomware attacks have been detected in hospitals and other test centres where the important files of the patients are taken and not returned till a particular amount of ransom is paid. Hospitals have been alerted about ransom sites that claim themselves to be government advised sites to keep a check on the corona patients but then hacks the system.

8. Other online crimes related to social media:
Social networking apps like Facebook, WhatsApp, Twitter have become an important tool to spread fake information. The Digital infrastructure across the globe is immensely comprised of these international tech-giants like YouTube, Google, Facebook, Twitter etc. The social world has witnessed a complete transformation by these corporations, without any regulation or accountability of their Modus Operandi. These fake news' triggers the people, as they blindly believe these reports, and start reacting accordingly. Besides this, these online chatting apps are misused to sexually harass people. It has become inevitable for the employees to stay in touch with each other, so they opt for these communication platforms and sometimes end up being exploited in some way or the other.

XII. DATA BREACH REPORT FOR THE YEAR 2020

A data breach is any incident where confidential or sensitive information has been accessed without permission. Breaches are the result of a cyberattack where criminals gain unauthorized access to a computer system or network and steal the private, sensitive, or confidential personal and financial data of the customers or users contained within. Healthcare is the most expensive industry for a data breach at $7.13 million, the global average cost of a data breach is $3.86 million and the average cost per lost or stolen record in a data breach is $150. Data breaches are becoming more and more common and some of the most recent data breaches have been the largest on record to date. Yahoo holds the record for the largest data breach of all time with 3 billion compromised accounts. Data breaches in 2020 decreased by 48% but the number of records exposed has exceeded 37 billion. In a security context, human error means unintentional actions - or lack of action - by employees and users that cause, spread or allow a security breach to take place. Based on the data breach quick view report released by 'Risk Based Security', there were 3,932 publicly reported breach events at the time of this report; a 48% decline compared to 2019. Despite 1,923 breaches (49%) without a confirmed number of records exposed, the total number of records compromised in 2020 exceeded 37 billion, a 141% increase compared to 2019 and by far the most records exposed in a single year.



Based on 2020 Year End Data Breach QuickView Report by Risk Based Security.

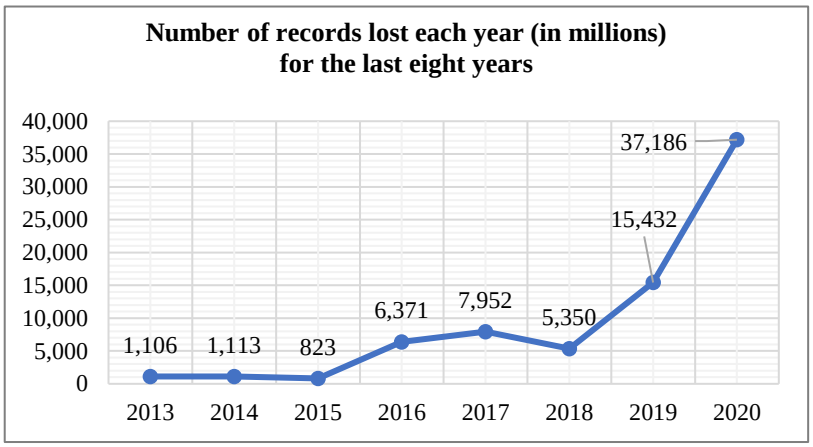
IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

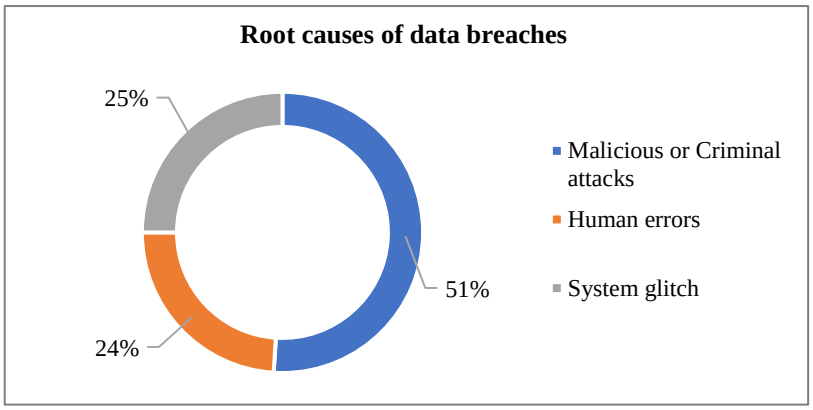
International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10443

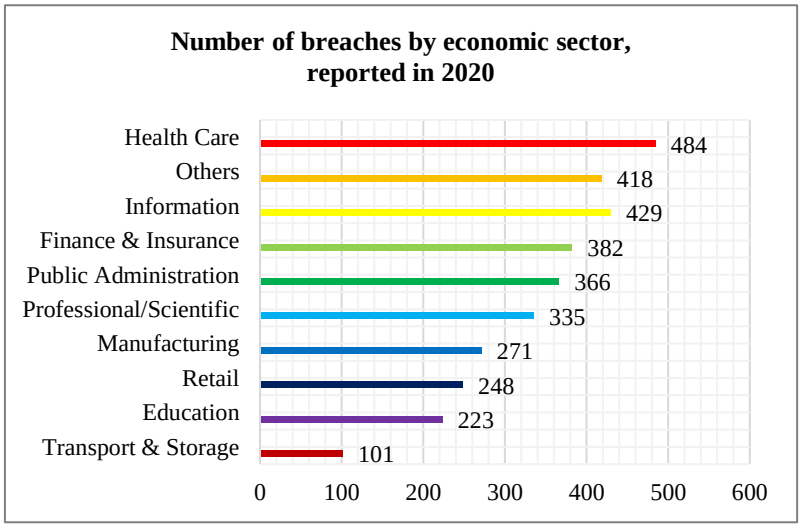


Based on 2020 Year End Data Breach QuickView Report by Risk Based Security.



Based on 2019 Cost of a Data Breach Report by IBM Security

There were 676 breaches that included ransomware as an element of the attack, a 100% increase compared to 2019. Five breaches each exposed one billion or more records and another 18 breaches exposed between 100 million and 1 billion records. Healthcare was the most victimized sector this year, accounting for 12.3% of reported breaches.



Based on 2020 Year End Data Breach QuickView Report by Risk Based Security.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10443

XIII. CYBER SECURITY AND SOLUTIONS FOR SECURITY THREATS

Cyber security is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyberattacks. It aims to reduce the risk of cyberattacks and protect against the unauthorised exploitation of systems, networks and technologies. Some of the important security techniques to counter the cyberattacks are:

1. Use Strong Passwords - Use different user ID and password combinations for different accounts, and avoid writing them down. Make the passwords more complicated by combining letters, numbers, special characters (minimum 10 characters in total) and change them on a regular basis.

2. Use Authentication - It is a process of identifying an individual and ensuring that the individual is the same who he/she claims to be. A typical method for authentication over internet is via username and password. With the increase in the reported cases of cybercrime by identity theft over internet, the organizations have made some additional arrangements for authentication like One Time Password(OTP), as the name suggest it is a password which can be used one time only and is sent to the user as an SMS or an email at the mobile number/email address that he have specified during the registration process. It is known as two-factor authentication method and requires two type of evidence to authentication an individual to provide an extra layer of security for authentication. Some other popular techniques for two-way authentication are: biometric data, physical token, etc. which are used in conjunction with username and password.

3. Use Encryption - It is a technique to convert the data in unreadable form before transmitting it over the internet. Only the person who have the access to the key and convert it in the readable form and read it. Formally encryption can be defined as a technique to lock the data by converting it to complex codes using mathematical algorithms. The code is so complex that it even the most powerful computer will take several years to break the code. This secure code can safely be transmitted over internet to the destination. The receiver, after receiving the data can decode it using the key. The decoding of the complex code to original text using key is known as decryption. If the same key is used to lock and unlock the data, it is known as symmetric key encryption. In asymmetric key encryption, the key used to encrypt and decrypt data are different. The asymmetric key encryption is also known as public key encryption.

4. Use Digital Signatures - A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions or digital messages. Signers can also use them to acknowledge informed consent. In many countries, including the United States, digital signatures are considered legally binding in the same way as traditional handwritten document signatures.

5. Use Anti-virus/Malware Software - There are verities of malicious programs like virus, worms, trojan horse, etc that are spread over internet to compromise the security of a computer either to destroy data stored into the computer or gain financial benefits by sniffing passwords etc. To prevent these malicious codes to enter to your system, a special program called an anti-virus is used which is designed to protect the system against virus. It not only prevents the malicious code to enter the system but also detects and destroys the malicious code that is already installed into the system. There are lots of new viruses coming every day. The antivirus program regularly updates its database and provides immunity to the system against these new viruses, worms, etc.

6. Activate your Firewall - It is a hardware/software which acts as a shield between an organization's network and the internet and protects it from the security threats. It can be used to limit the persons who can have access to your network and send information to you. A firewall can be implemented using hardware as well as software or the combination of both. Example of hardware firewalls are routers through which the network is connected to the network outside the organization i.e. Internet and the software firewalls are installed and installed on the server and client machines and it acts as a gateway to the organization's network.

7. Use Steganography - It is a technique of hiding secret messages in a document file, image file, and program or protocol etc. such that the embedded message is invisible and can be retrieved using special software. Only the sender and the receiver know about the existence of the secret message in the image. The advantage of this technique is that these files are not easily suspected. There are many applications of steganography which includes sending secret

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10443

messages without ringing the alarms, preventing secret files from unauthorized and accidental access and theft , digital watermarks for IPR issues, etc.

8. Block spyware attacks - Prevent spyware from infiltrating your computer by installing and updating anti-spyware software on a regular basis.

9. Be Social Media Savvy - Make sure your social networking profiles (e.g. Facebook, Twitter, YouTube, MSN, etc.) are set to private. Check your security settings. Be careful what information you post online.

10. Secure your Mobile Devices - Be aware that your mobile device is vulnerable to viruses and hackers. Download applications from trusted sources.

11. Install the latest operating system updates - Keep your applications and operating system (e.g. Windows, Mac, Linux) current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.

12. Secure your wireless network - Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Public Wi-Fi or Hotspots, are also vulnerable. Avoid conducting financial or corporate transactions on these networks.

13. Protect your e-identity - Be cautious when giving out personal information such as your name, address, phone number or financial information on the internet. Make sure that websites are secure while making online purchases.

14. Avoid being scammed - Always think before you click on a link or file of unknown origin. Do not feel pressured by any emails. Check the source of the message. When in doubt, verify the source. Never reply to emails that ask you to verify your information or confirm your user ID or password.

15. Call the right person for help – Do not panic if you are a victim. If you encounter illegal internet content (e.g. child exploitation) or if you suspect a computer crime, identity theft or a commercial scam, report this to your local police. If you need help with maintenance or software installation on your computer, consult with your internet service provider or a certified computer technician.

16. Protect your Data - Use encryption for your most sensitive files such as tax returns or financial records, make regular backups of all your important data, and store it in another location.

XIV. CONCLUSION

"Prevention is better than cure" - We are living in the modern era run by technology. Our daily life depends on it, live with it. As internet usage is increasing day by day, it makes the world small; people are getting closer to the cyber attackers who performs various cybercrimes. During COVID-19 pandemic, cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation around the world. At the same time, the higher dependency on connectivity and digital infrastructure due to the global lockdown increases the opportunities for cyber intrusion and attacks. One of the best ways to stop these criminals and protect sensitive information is by making use of highly standard security software and hardware to prevent our system from cyberattacks. Awareness and Education of cybercrimes, cyber law and cyber security is must necessary, which helps people to gain knowledge about it and to prevent themselves from being the victim to various cybercrimes and attacks in advance in this modern technology world.

REFERENCES

[1]. Kamini Dashora (2011), "Cyber Crime in the Society: Problems and Preventions", Journal of Alternative Perspectives in the Social Sciences, 3(1), pp. 240-259.
[2]. P. N. V. Kumar, "Growing cyber crimes in India: A survey," 2016 International Conference on Data Mining and Advanced Computing (SAPIENCE), 2016, pp. 246-251, doi: 10.1109/SAPIENCE.2016.7684146.
[3]. Dr. Jeetendra Pande, "Introduction to Cyber Security" [Online], Uttarakhand Open University Available at: https://uou.ac.in/sites/default/files/slm/Introduction-cyber-security.pdf
[4]. Paolo Passeri (2020), "2019 Cyber Attacks Statistics", Available at: https://www.hackmageddon.com/2020/01/23/2019-cyberattacks-statistics/
[5]. Paolo Passeri (2021), "2020 Cyber Attacks Statistics", Available at: https://www.hackmageddon.com/2021/01/13/2020-cyberattacks-statistics/
[6]. Ravi Bandakkanavar (2020), "Causes of CyberCrime and Preventive Measures", Available at: https://krazytech.com/technical-papers/cybercrime

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10443

[7]. Nikola Zlatanov (2015), "Computer Security and Mobile Security Challenges".
[8]. "6 TYPES OF HACKERS", Available at: https://ifflab.org/6-types-of-hackers/
[9]. "Hacker Hat Colors: An Inside Look at the Hacking Ecosystem", Available at: https://alpinesecurity.com/blog/hacker-hat-colors-an-inside-look-at-the-hacking-ecosystem/
[10]. "Cyber Crime: How You Can Prevent It!", Available at: https://www.ccplus-usa.com/cybercrime-can-prevent/
[11]. Mike Chapple, "Confidentiality, Integrity And Availability – The CIA Triad", Available at: https://www.certmike.com/confidentiality-integrity-and-availability-the-cia-triad/
[12]. UKEssays (November 2018), "Cyber Crimes and Cyber Security", Available at: https://www.ukessays.com/essays/information-technology/cybercrimes-cyber-security-1836.php?vref=1
[13]. INTERPOL, "COVID-19 cyberthreats", Available at: https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats
[14]. Mary K. Pratt, "cyber attack", Available at: https://searchsecurity.techtarget.com/definition/cyberattack
[15]. "Cybercriminals", Available at: https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals
[16]. "What is a DDoS Attack? - DDoS Meaning", Available at: https://www.kaspersky.co.in/resource-center/threats/ddos-attacks
[17]. Ian Mitch, Elizabeth Bodine-Baron, "Cyber Warfare", Available at: https://www.rand.org/topics/cyber-warfare.html
[18]. Kameswar Lenka (2017), "Precautionary measures to prevent cyber crime."[Online], Available at: https://www.coursehero.com/file/32443780/cybercrimesdocx/
[19]. Ridhima and Arshdeep Singh (2020), "Growth in Cybercrimes in the COVID-19 times and Fragile Cyber Laws in India", Available at: https://www.latestlaws.com/articles/growth-in-cybercrimes-in-the-covid-19-times-and-fragile-cyber-laws-in-india/
[20]. Mr Adil Radoini, "Cybercrime during the COVID-19 Pandemic", Available at: http://f3magazine.unicri.it/?p=2085
[21]. INTERPOL (2020), "INTERPOL report shows alarming rate of cyberattacks during COVID-19", Available at: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19
[22]. "What is a hacker?", Available at: https://www.webroot.com/in/en/resources/glossary/what-is-a-hacker
[23]. "What is Cyber Security?", Available at: https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security
[24]. Ben Lutkevich, "What is Cyber Security?", Available at: https://searchsecurity.techtarget.com/definition/digital-signature
[25]. "What is Social Engineering? Examples & Prevention Tips", Available at: https://www.webroot.com/in/en/resources/tips-articles/what-is-social-engineering
[26]. Madelyn Bacon, "hacktivism", Available at: https://searchsecurity.techtarget.com/definition/hacktivism
[27]. "Heightened threat scenario: all the facts in the AV-TEST Security Report 2018/2019", Available at: https://www.av-test.org/en/news/heightened-threat-scenario-all-the-facts-in-the-av-test-security-report-2018-2019/
[28]. "PSW Trojans (Password-stealing Trojans)", Available at: https://encyclopedia.kaspersky.com/glossary/psw-trojans-password-stealing-trojans/
[29]. "Spamming", Available at: https://simple.wikipedia.org/wiki/Spamming
[30]. "Backdoor Attack", Available at: https://www.imperva.com/learn/application-security/backdoor-shell-attack/
[31]. Dan Lohrmann (2021), "2020 Data Breaches Point to Cybersecurity Trends for 2021", Available at: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-data-breaches-point-to-cybersecurity-trends-for-2021.html
[32]. Bhavna Arora, "Exploring and analyzing Internet crimes and their behaviours", Available at: https://www.sciencedirect.com/science/article/pii/S2213020916301537
[33]. Micke Ahola, "The Role of Human Error in Successful Cyber Security Breaches", Available at: https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches
[34]. Larry Ponemon (2019), "What's New in the 2019 Cost of a Data Breach Report", Available at: https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/
[35]. "What is Cyber Security? Definition and Best Practices", Available at: https://www.itgovernance.co.uk/what-is-cybersecurity
[36]. "2021 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends", Available at: https://purplesec.us/resources/cyber-security-statistics/
[37]. Inga Goddijn and The Cyber Risk Analytics Research Team-Risk Based Security (2021), "2020 Year End Data Breach QuickView Report", Available at: https://pages.riskbasedsecurity.com/hubfs/Reports/2020/
[38]. Harris Insights & Analytics Market research company (2020), "2019 NortonLifeLock Cyber Safety Insights Report", Available at: https://www.nortonlifelock.com/content/dam/nortonlifelock/pdfs/reports/2019-nortonlifelock%20-cyber-safety-insights-report-global-results-en.pdf