Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Challenges for Cyber Security and Trends on Recent Technologies

Dr Maheshwari*
Dept. of CSE
Amrita School of Engineering,
Chennai, India
a_maheshwari@ch.amrita.edu
Mr. Ravi Venkat Jayanth
Dept. of CSE
Amrita School of Engineering,
Chennai, India
rvjayanth1111@gmail.com

Mr. Peyyala Sahith Venkata Krishna
Dept. of CSE
Amrita School of Engineering,
Chennai, India
sahithpeyyala68@gmail.com

Mr. Vanapalli Jaitesh Balaji
Dept. of CSE
Amrita School of Engineering,
Chennai, India
jaitesh98@gmail.com
Mr. Dondeti Venkata Krishna Reddy
Dept. of CSE
Amrita School of Engineering,
Chennai, India
venkatakrishna9642@gmail.com

Article Info
Page Number: 134-141
Publication Issue:
Vol 71 No. 3s2 (2022)

Article History
Article Received: 28 April 2022
Revised: 15 May 2022
Accepted: 20 June 2022
Publication: 21 July 2022

Abstract
In the technology world, cyber security is very important. In the current situation, security for information shared on social media sites has become a major issue. Cyber Crimes are becoming more prevalent globally. Various governments are working together to combat these types of crimes. This paper mainly focuses on the new trends raised in modern time, techniques to avoid cybercrimes, ethics and also the how social media affects the cyber security.
Keywords: - cyber security, cyber-crimes, malwares, cyber ethics, social media, firewalls, cloud services.

Introduction

The usage of internet is becoming more popular in India. As the internet can be used for the good thinks like learning stuff from internet and connecting people but there is a flip side of this coin where

people use internet to do bad stuff like collecting data from a person and using it for their own good. Cyber-crime is a crime in which people use a computer and the internet to steal public identity or illegal imports from browsers or through malicious programs. Cyber-crime is an activity done using internet and the computers or laptop. Cybersecurity is the process or steps taken to save the people from the cyber-attacks and save their data from being stolen. So cyber

security is important for every computer, mobiles, servers and organisations. The main aim of

cyber security is to establish rules and measure to use against attacks over the internet.

Even the latest technologies like cloud computing, net banking, online transactions and E-commerce etc. We need a high-level security for this kind of technologies. As we all know, this type of technology contains highly sensitive information, thus security must be a top priority. Cyber security is very important for the well-being of any country. It can be improved through the use of various technologies such as cloud computing and online transactions. A more secure method is required to overcome cybercrimes.

Many countries and organizations have already implemented strong security policies to prevent the loss of sensitive data.

According to recent reports India made it to the top 10 in Global Cybersecurity Index 2020 by International Telecommunication Union, moving up 37 places to rank as the 10-best country in the world on key cyber safety parameters. Some what we are stepped up in terms of security. And also, India has been ranked 4^{th} in the Global Cybersecurity Index 2020 in the Asia-Pacific region with an overall score of 97.49.

Cyber Crime

The United States Justice Department has expanded the definition of cybercrime. Cybercrime is defined as to include illegal behaviour involving the use of a computer to save evidence. Cybercrime is a term that refers to any illegal action that involves the use of a computer as the primary means of commissioning or stealing. Cybercrime includes various types of crimes, such as network intrusions, extortion, and identity theft. It had become a big issue globally. Cybercrime is often characterised like a crime involving the use of computing device in order to steal an individuals appearance or sell their pornography, or to annoy and disturb victims' activities via malicious programmes. Because technology plays such an important role in people's lives on a daily basis. Cybercrime will continue to grow as technology advances.

Cybersecurity Methods

A. Control of Access and Password Protection

The usernames and passwords approach has evolved into a critical component of data security. One of the first cyber security measures might be this. Before uploading, we must ensure that the reports we acquire are from a reliable and trustworthy source and that they have not been altered. In order to protect computers from viruses, effective antivirus software is required.

B. Malware scanners

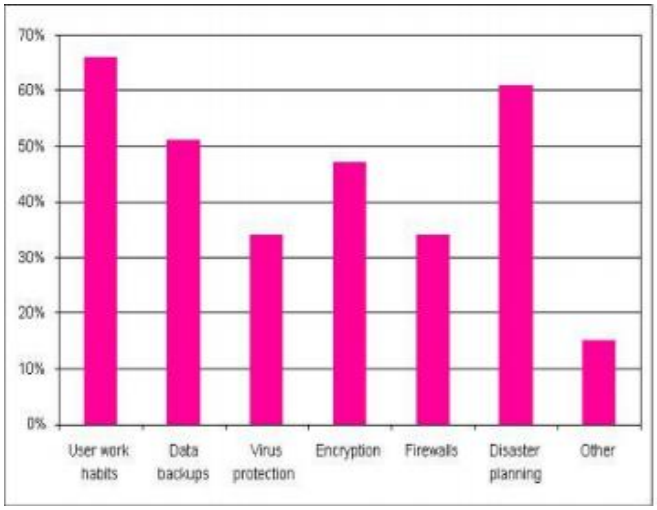
The application checks all data and documents stored on the device for dangerous code or fatal viruses on a regular basis. Malicious software includes viruses, worms, and trojan horses, which are sometimes mixed together and referred to as malware.

C. Firewalls

A firewall is a piece of software or hardware programme that protects your computer from attacks from the outside world. It helps detect viruses, malware, and internet-based worms that try to infect a machine. The current firewall examines all communications entering or exiting the Internet, and those that do not fit the predefined security requirements are blocked.

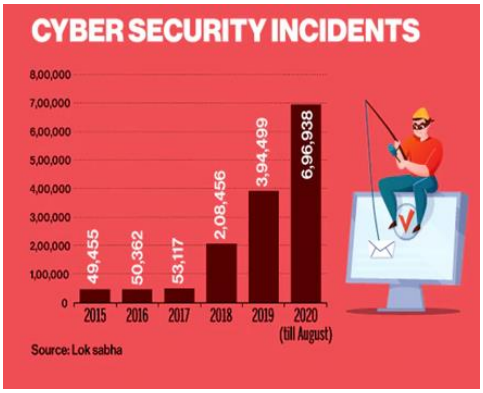
D. Anti-virus software

Antivirus software is a piece of software that detects, prevents, and actively works to disable or destroy computer viruses and worms. Many antivirus programmes include an auto-update feature that allows the system to automatically download new virus types and check that they are recognised. Antivirus software is an absolute requirement for any device.



Cybersecurity:

Every company's data security and privacy will always be a top focus. We currently live in a digital or electronic world where all data is saved. Cyber attackers will continue to attack social networking sites for the purpose of stealing personal information from ordinary individuals.



A person must take all required precautions not just when using social media, but also when using a bank.

There are number of factors that increase in cyber security incidents recently. During the pandemic organizations some were figuring out how to continue doing business and people were connecting through remote locations, sometimes using their personal devices, which made hackers easy to active. Further, this has impacted employment in so many ways across the world, in terms of increased hacking activity.

Trends changing cyber security:

1.Work from home:

As the covid-19 pandemic caused many organisations to stay closed for the public safety. To make their organisations operational the companies have opted for work for home scheme. So, most of the employees are using their personal computers and personal Wi-fi networks which lack the protection of the centralized offices which usually have secure firewalls and routers.

As many employees are using their mobiles to communicate with their team members, they will have instant messaging clients like Microsoft teams or zoom. And these made the lines between professional and personal life blurred it increases the risk of sensitive information is kept open for hackers.

So, this is a critical cyber security trend to focus on for organisations to run their business securely by improving system security, implementing security controls and by ensuring proper documentation and monitoring.

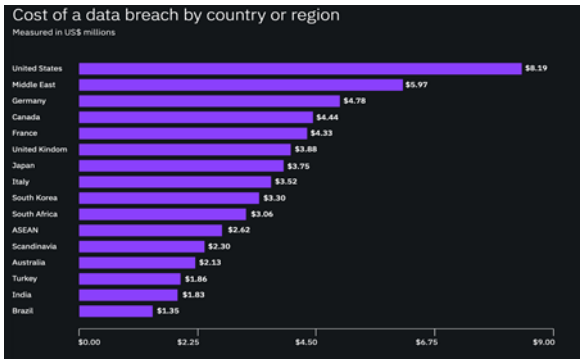
2.Increase in cloud services:

As most of the people are shifting to cloud services the cloud vulnerability is becoming one of the biggest cyber security trends. Even though the people have been migrating to cloud services before the pandemic has helped as a catalyst as the business and schools are using online services to keep business and education running.

The cloud services offer efficient and cost saving methods for any service so many people are opting for cloud services and so do the hackers. Misconfigured cloud security setting is the main cause for the cyber-attacks and data breaches and unauthorised access. On average 3.86 million dollars are lost due to data breaches so the organisations should take steps to minimise the loss.

3.The raise in use of Artificial Intelligence:

As the security threats are becoming too much for humans to handle so the organisations are turning towards AI and machine learning maintain their infrastructure.



AI can analyse massive quantity of data at risk much faster than a human can do which is beneficial for large scale and small-scale organisations to detect the threat and solve it on average a fully developed AI model saved an average of 3.58 million dollars in the year 2020.

With AI the organisations can have robust and accurate threat detection among the companies and the bad guys are using data poisoning and model stealing to take advantage of this tech and automate their cyber-attacks.

Social media's role in cyber security:

Social media is a platform which helps the people to communicate with each other and share the personal data. So as a result, in terms of personal cyber security threats, social media plays a significant role. There is a great importance for security for anyone who is using a computer or a mobile device or an organization the uses computers on daily bases. As we know, the social media platforms like Facebook, Twitter and WhatsApp have changed their platforms on how people use their accounts for professional and personal use.

These are some of the ways the social media sabotages your cyber security.

1. Providing personal information:

If your account isn't set to private the stuff like our date of birth, native place, schools you attended to, family photos are left open and any one can access that information. Identity thieves can use this information to break into your account or apply credit card with the info you provided in your social media so avoid sharing too much of your personal data in social media.

2.Info shared by employees:

As most of the employees have a social media account, they tend to share the info on the project they are working on or photos form the work place, they might end up sharing more than what they should and can hurt your business.

3. Malware:

One of the most common entry points for malware is social networking. The most common types of malwares are download links and emails, which can also be spread as promotions or shortened links, and which can be used to steal personal files and banking information.

4. Unused social media accounts:

Unused social media accounts can be hacked by the hackers and used to commit fraud, post illegal content, spread inappropriate messages and all sorts of bad things under your name.

Cyber ethics

The code of the internet is known as cyber ethics. We have a high probability of using the internet if we follow these cyber ethics in a proper and secure manner.

Here are a few examples:

1. The Internet is widely recognised as the world's largest library, It is important to utilise this knowledge, which contains information on practically every subject in any discipline in an extremely accurate and timely manner. The use of legal methods is frequently required.

2. Do not use other people's passwords to access their accounts.

3. Do not call someone a name, tell a falsehood about them, show them humiliating photos or do something else you can think of to wreak devastation on them.

4. DO communicate and engage with others via the Internet. Communication is straightforward using email and instant messaging. Maintain contact with relatives and friends, as well as family members, and speak with co-workers with whom you can exchange ideas and sharing information with folks from all over town or half-way across the globe.

5. Sending viruses to other people's machines is never a good idea.

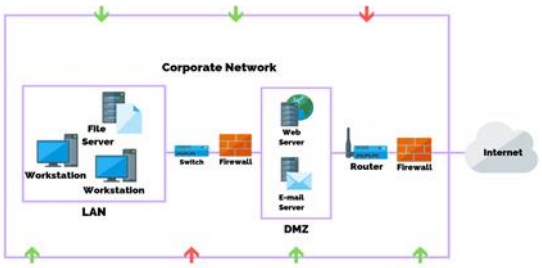
6. Never pretend to be someone else online, and never create bogus accounts for others other people since you'll end up in the same situation causing trouble for the other person.

7. Never give out your personal data to anyone since there is a high probability that it may be misused by others and that you will be harmed as a result.

8. Always protect copyrighted content and only download games or videos if doing so is legal

9. Consumers and businesses will improve their resilience and sensitivity in order to protect themselves from various risks or to mitigate the potential effects of accidents by employing necessary countermeasures and adopting outstanding Internet security procedures. As needed, configure and modify operating system components and other computer programmes. Security systems, anti-virus, and anti-spyware software are all regularly used and updated. It could become an object of identity or assets depending on the info you submit.

The previous are some cyber ethics to observe when utilizing the internet. We have always been taught good rules from a young age. We employ the same principle in cyberspace.



Conclusion:

As the world is getting increasingly connected through networks computer security is becoming increasing relevant. Crucial transactions are being done using this every year new type of cybercrime and new type of information security is being developed.it is becoming increasing challenging for the organizations to defend their infrastructure from cybercrime and also how they have to invest in new platforms and intelligence to do so, which are mostly caused by the disruptive technologies and new cyber threats that emerge every day while there is no ideal solution for the cybercrime, We should try in every possible way to fight against cyberthreats to keep our cyberspace safe and secure.

References:

1. Computer Security Practices in Non-Profit Organisations – A Net Action Report by Audrie Krause.
2. Nina Godbole and Sunit Belapure (2011), "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", New Delhi, Wiley India Pvt Ltd. SBN-13: 978-8126521791 ISBN-10: 9788126521791
3. Booz Allen and Hamilton, Reports, "Top Ten Cyber Security Trends for Financial Services", 2012
4. Luis corrons – Panda Labs (2013) A Look back on Cyber Security 2012.
5. IEEE Security and Privacy Magazine – IEEECS —Safety Critical Systems – Next Generation —July/ Aug 2013.
6. Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole
7. Kellermann, "Technology Risk Checklist, Cybercrime and Security", IIB-2
8. www.hackmageddon.com/2019/04/17/march-2019-cyber-attacksstatistics/.
9. "U.S. Health Agency Suffers Cyber-Attack During COVID-19 Response," 2020, https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response.
10. Ajitha, P.Sivasangari, A.Gomathi, R.M.Indira, K."Prediction of customer plan using churn analysis for telecom industry",Recent Advances in Computer Science and Communications,Volume 13, Issue 5, 2020, Pages 926-929.
11. "Sivasangari A, Ajitha P, Rajkumar and Poonguzhali," Emotion recognition system for autism disordered people", Journal of Ambient Intelligence and Humanized Computing (2019)."
12. Ajitha, P., Lavanya Chowdary, J., Joshika, K., Sivasangari, A., Gomathi, R.M., "Third Vision for Women Using Deep Learning Techniques", 4th International Conference on Computer, Communication and Signal Processing, ICCCSP 2020, 2020, 9315196
13. Sivasangari, A., Gomathi, R.M., Ajitha, P., Anandhi (2020), Data fusion in smart transport using convolutional neural network", Journal of Green Engineering, 2020, 10(10), pp. 8512–8523.

14. A Sivasangari, P Ajitha, RM Gomathi, "Light weight security scheme in wireless body area sensor network using logistic chaotic scheme", International Journal of Networking and Virtual Organisations, 22(4), PP.433-444, 2020
15. Sivasangari A, Bhowal S, Subhashini R "Secure encryption in wireless body sensor networks",Advances in Intelligent Systems and Computing, 2019, 814, pp. 679–686
16. Sindhu K, Subhashini R, Gowri S, Vimali JS, "A Women Safety Portable Hidden camera detector and jammer", Proceedings of the 3rd International Conference on Communication and Electronics Systems, ICCES 2018, 2018, pp. 1187–1189, 8724066.
17. Gowri, S., and J. Jabez. "Novel Methodology of Data Management in Ad Hoc Network Formulated Using Nanosensors for Detection of Industrial Pollutants." In International Conference on Computational Intelligence, Communications, and Business Analytics, pp. 206-216. Springer, Singapore, 2017.
18. Gowri, S. and Divya, G., 2015, February. Automation of garden tools monitored using mobile application. In International Confernce on Innovation Information in Computing Technologies (pp. 1-6). IEEE.