JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

CYBER SECURITY (THREATS & SOLUTION)

[1]Name of First Author: Sandeep Kaur, [2]Name of Second Author: Sukhdeep Singh

[1]Assistant Professor in Computer Science, [2]Assistant Professor in Mathematics
Miri Piri Khalsa College, Bhadaur, India

Abstract: Cyber security systems are the protection of networks and data from digital attacks, theft or loss. As cyber threats evolve, they include malicious activities such as hacking, phishing, ransomware, and data breaches. These attacks mostly target individuals, organizations and governments, often seeking access to sensitive information for financial or disruptive purposes.

Increasing reliance on technology and the interconnectedness of devices through the Internet of Things (IoT) has increased the potential attack surface. As the result cyber security is playing an important role in maintaining personal security, protecting business assets and maintaining national security. Technologies like encryption, firewalls, multi-factor authentication, and intrusion detection systems are used to find cyber threats.

Many cybersecurity measures advance, so do the techniques used by attackers, leading to an ongoing arms race in digital security. Organizations are taking proactive measures to reduce risks, including training employees, conducting regular security audits, and incident response plans. Additionally, the integration of artificial intelligence and machine learning is helping to identify and counter threats. In this digital age, cybersecurity is essential, requiring constant innovation and vigilance to stay ahead of an ever-evolving threat landscape.

INTRODUCTION:

Cybersecurity is a broad field that deals with protecting networks, systems and data from online threats. In today's global village, in this interconnected world where information is critical to businesses and individuals, the importance of cyber security cannot be ignored. This cyber security includes a wide range of technologies whose main purpose is to protect digitally existing assets from cyber threats. Its function includes preventing unauthorized access to data, and potential breaches. At its core, cyber security follows the principle of security in depth. What kind of efforts are made to reduce risks and eliminate deficiencies and security controls. Firewalls, encryption setting, virus detection software plays important role in cyber security. For enhancing cyber security working on malware, phishing, ransomware, and social engineering strategies to detect, prevent, and respond to various cyber threats is very necessary. Cyber security awareness and training also play an important role. Technology is increased and the attack of cyber threats are also growing. To prevent data from cyber attacks we need experienced and qualified cyber security experts who can help protect the data held digitally and maintain privacy so that people can feel confident and they work digitally.

CYBER CRIME:

Digital wrongdoing refers to any illegal activity that centers around using a computer for its primary method of execution and theft. The U.S. Department of Justice broadens the definition of cybercrime to cover any criminal behaviour that involves a computer as a tool for storing evidence. The expanding range of cyber offenses includes crimes facilitated by computers, such as network disruptions and the proliferation of computer viruses, as well as computer-based versions of existing crimes like identity theft, tracking, bullying, and cyberbullying, which have become significant concerns for individuals and nations. In simple language, cybercrime is defined as crimes committed using computers and the Internet to steal someone's personal data, sell the stolen data, digitally track a person's activities, or interfere with work with malicious programs such as viruses. Goes Technology is playing an important role in people's lives and the use of technology is increasing Day by day but cyber crimes are on the rise across the country. Silicon Valley Bank noted that cyber attacks are being viewed as a serious threat by technology companies. This is a threat to both their data and their business operations.

PHISHING:

Hackers steal people's sensitive and personal information such as email, banking passwords and other financial details and then use them to commit fraud. Phishing hackers not only target the general public but also various sectors including banking and government agencies. According to a report by ET CISO, India ranks second globally in phishing attacks with over 2.29 billion incidents in 2022.

RANSOMWARE:

Ransomware attack encrypts a person's data and demands payment to return it. Ransomware incidents have increased day by day in India, affecting businesses, hospitals and government institutions.

DISTRIBUTED DENIAL OF SERVICE (DDOS):

DDoS attacks overwhelm a target server with traffic, disrupting its services. In India, DDoS attacks have targeted financial institutions, media outlets and government websites. DDoS attacks increased significantly during the Covid-19 pandemic in the country, recording a 300% increase in April 2020 compared to the previous year.

DATA BREACHES:

These involve the unauthorized access and theft or exposure of sensitive and personal data. In the past years India has experienced several high-profile data breaches, affecting millions of people. For example, the 2019 breach of Indian airline Spice Jet exposed the personal information of more than 1.2 million passengers.

MALWARE:

Some malicious software and programs are specially designed to steal data from computers and other digital systems, interrupted in operations, or get unauthorized access. India faces a constant threat from malware because new malware is being created daily. These malwares target both individuals and organizations.

CYBER THEFT:

Unauthorized access of any digital information with the intent to steal sensitive and personal information or financial resources is called cyber theft. Cyber theft incidents in India are increased, with significant growth in financial fraud through digital medium. According to the report of Reserve Bank of India (RBI), the number of cyber crime incidents reported in the banking sector alone has increased by 3.5 times from 2015 to 2018. According to the National Crime Records Bureau (NCRB), in 2020, cybercrime cases in India increased by 300%, with financial fraud being the most common type. According to the report published in 2024, a total of 1128265 cases have been reported in a year.

WEB JACKING:

Web jacking, also known as website defacement. It involves unauthorized intervention for some changes in the content of the website. Some do this for political or ideological reasons. India has seen many incidents of web jacking, targeting government websites and high-profile corporate sites. According to the Ministry of Electronics and Information Technology, approximately 373 government websites were hacked in 2023 in India. Web site hacking incidents can cause serious damage to well-known organizations, causing damage to their reputation and loss of trust among users.

SPAM:

Unwanted and malicious emails and messages in bulk is called spam. These messages are typically sent for advertising, phishing, or spreading malware. India is the largest generator of spam emails globally. A significant portion of which stems from compromised systems within the country. According to sophops report India is ranked third in the world for the most spam sending systems. Spam email is not only a nuisance, but also a security risk. It can be used to distribute malware or trick users into disclosing sensitive information.

LOGIC BOMB:

A logic bomb is a type of virus code that planted inside a system to target specific task or condition. It executes harmful effects and track systems activities. Logic bomb's exact statistics data not available in India but incidents of insider threats and sabotage have been reported in various industries. A employee of a famous Indian IT company planted a logic bomb in the company's systems after leaving the company in 2018.

CHILD PORNOGRAPHY:

Child pornography is the making of indecent sexual images or videos of minors and forwarding these images or videos through various media. It is a serious criminal offense. India has seen an alarming rise in cases of online child sexual exploitation material (CSAM) in recent years. According to the National Crime Records Bureau (NCRB), 450207 cyber crimes reported against children pornography in India in year 2023. Law enforcement agencies and child rights organizations in India are working together to combat the spread of child pornography through increased surveillance and public awareness campaigns.

Each of these cyber-attacks poses unique challenges to cyber security in India, requiring large-scale strategies to effectively prevent, detect and respond to such threats.

THESE ARE SOME TIPS TO PREVENT YOURSELF FROM CYBER ATTACKS:

USE STRONG PASSWORDS:

Create strong and unique passwords for each of your online accounts so that no one else can access them. Create a password using a combination of upper and lower case letters, numbers and special characters. Always use a trusted password manager to securely store and manage your passwords.

TWO-FACTOR AUTHENTICATION (2FA):

Enable 2FA whenever possible, especially for sensitive accounts like email, banking and social media. This adds an extra layer of security to any account, just like a code sent to your phone.

KEEP SOFTWARE UPDATED:

Regularly update your operating system, software applications, and antivirus programs to patch known vulnerabilities. Cyber attackers often attack on outdated software to gain unauthorized access to systems.

BEWARE OF PHISHING ATTACKS:

Beware of any unsolicited emails, messages or calls asking you for personal or financial information. Avoid clicking on unknown sources or links or downloading attachments. Verify the validity of emails by checking the sender's email address and checking the content for spelling errors or unusual requests.

PRACTICE SAFE BROWSING HABITS:

Visit only reputable websites with HTTPS encryption to protect your data in transit. Avoid clicking on suspicious links or pop-up ads, as these may lead to malware infection. Consider using a virtual private network (VPN) when accessing the Internet from public Wi-Fi networks to encrypt your connection and protect your privacy.

PROTECT YOUR DEVICES:

Install a good and reputed antivirus and anti-malware software on all your devices, computers, smartphones and tablets. Enable device encryption to protect data stored on your devices in case they are lost or stolen.

BACK UP YOUR DATA TIME TO TIME:

Back up your important files and data regularly to an external hard drive, cloud storage, network-attached storage (NAS) or any secure storage device. In case you lost your data in a cyber attack or data breach, then you can recover your files.

EDUCATE YOURSELF AND OTHERS:

Stay up-to-date about the latest cybersecurity threats and trends by searching about new resources. We should also attending cybersecurity awareness programs. We beware from cyber attacks and also educate our family members, friends and colleagues about cyber security so that they can live safely.

REPORT SUSPICIOUS ACTIVITY:

While we are searching on internet and we see any suspicious or dangerous activity, we should immediately report it and complaints about that to the relevant authorities. Crime branch also help us to track these dangerous activities.

By following these tips we can reduce the risk of cyber attacks and protect our personal and sensitive information.

CONCLUSION:

Cyber security is essential to protecting digital assets, personal data, and national infrastructure. As cyber threats continue to grow in complexity, individuals, organizations and governments must take proactive measures. This includes advanced encryption, multi-layered security protocols, and employee training. Collaboration across sectors and countries is critical to addressing security vulnerabilities and mitigating potential risks. Investing in cyber security not only protects sensitive information but also builds trust and resilience in the digital ecosystem. Technology advancements, constant research, adaptation, and vigilance are paramount to countering cyber threats and ensuring a secure cyber environment.

REFERENCE:

1. A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.
2. Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole
3. Computer Security Practices in Non Profit Organisations – A NetAction Report By Audrie Krause.
4. A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.
5. International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518, "Study of Cloud Computing in HealthCare Industry " by G.Nikhita Reddy, G.J.Ugander Reddy