IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, June 2023

Enhancing Cyber Security Awareness for Students

Pratibha Tambewagh
Lecturer, ME Computers
Bharati Vidyapeeth Institute of Technology, Kharghar, Navi Mumbai, India

Abstract: *In today's interconnected world, cyber threats have become a significant concern for individuals, organizations, and governments. With the increasing sophistication of cyber attacks, it is essential to develop a strong foundation of cyber security awareness among users,students. This paper explores the importance of cyber security awareness and provides insights into effective strategies to enhance it. By fostering a culture of cyber security awareness, individuals and organizations can better protect themselves from potential threats and contribute to a safer digital environment.*

Keywords: Cyber Security, Cyber-attacks, Denial of Service (DoS)

I. INTRODUCTION

The rapid growth of technology and the digital landscape has brought numerous benefits, but it has also exposed individuals and organizations to various cyber threats. Cyber criminals constantly devise new methods to exploit vulnerabilities and gain unauthorized access to sensitive information. To counter these threats, the development of cyber security awareness is crucial. This paper examines the significance of cyber security awareness and presents an overview of its various aspects.benefited byanonymous providing information to the media, free speech, talking to unknown people on social media and giving confidential information. Some people are making money by spreading fake news and the security of the country is deteriorating .

II. LITERATURE SURVEY

The biggest cyber security threats are Phishing, Ransomware, Botnet, DoS attack, social engineering attack, Cryptocurrency hijacking. These attacks are done for fraud, exploitation, extortion, causing disrepute and for personal revenge.

1. Why is Cyber Security Awareness Important in Today's Digital World?

Cyber security awareness is crucial in today's digital world because of the increasing reliance on technology and the widespread use of the internet.

Cyber threats, such as cyber attacks, data breaches, identity theft, and online scams, are constantly evolving and can have severe consequences for individuals, organizations, and even societies.Lack of awareness and knowledge about cyber security can make individuals vulnerable to these threats, resulting in financial losses, reputational damage, and emotional distress. With the proliferation of social media, online communication, and e-commerce, personal information is being shared and stored online more than ever, making it imperative to understand how to protect it.

Cyber security awareness helps individuals make informed decisions, develop safe online practices, and protect themselves from cyber threats, thus safeguarding their digital lives and ensuring a secure online experience. Additionally, cyber security awareness is important for students as they grow up in a digital-first world and need to develop responsible and safe online behaviors from a young age. By being aware of cyber security best practices, students can become responsible digital citizens and protect themselves and their online assets, now and in the future.

2. What is Cyber Security?

Cyber security is the practice of protecting digital devices, systems, and networks from cyber threats.It involves the implementation of measures, processes, and best practices to safeguard the confidentiality, integrity, and availability of digital assets.Cyber security encompasses a wide range of technologies, practices, and policies designed to defend against various types of cyber threats, such as cyber attacks, data breaches, malware, ransomware, phishing, social engineering, and more.The goal of cyber security is to prevent unauthorized access, disruption, or damage to digital

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, June 2023

assets, and to ensure the privacy, security, and trustworthiness of online information and communication.Cyber security is an ongoing process that requires continuous monitoring, updates, and adaptation to the evolving threat landscape in order to effectively mitigate risks and protect against cyber threats.

3. Common Cyber Threats

Cyber threats are malicious activities that target digital devices, systems, networks, and individuals with the intent of causing harm, stealing information, or disrupting operations.There are various types of cyber threats that can pose risks to individuals and organizations, including:

Cyber Attacks: These are deliberate attempts to exploit vulnerabilities in digital systems or networks, disrupt operations, steal or manipulate data, or gain unauthorized access to sensitive information. Examples of cyber attacks include malware attacks, denial-of-service (DoS) attacks, ransomware attacks, and phishing attacks.

Cyber Bullying: This refers to the use of technology, such as social media, email, or messaging, to harass, intimidate, or humiliate individuals online. Cyber bullying can involve spreading rumors, sending threatening messages, sharing personal information without consent, or posting hurtful comments or images.

Identity Theft: This occurs when someone steals personal information, such as names, addresses, social security numbers, or financial details, to impersonate individuals and commit fraud or other criminal activities. Identity theft can result in financial loss, reputational damage, and legal consequences.

Social Engineering: This involves manipulating individuals into revealing sensitive information or performing actions that compromise security. Social engineering techniques can include phishing, pretexting, baiting, and other methods that exploit human vulnerabilities and trust.

It's important to be aware of these common cyber threats and take appropriate measures to protect against them, including implementing security measures, using strong and unique passwords, being cautious online, and reporting any suspicious activities to relevant authorities.

4. Examples of Common Cyber Threats

Phishing: Phishing is a type of cyber attack where attackers try to trick individuals into revealing sensitive information, such as usernames, passwords, credit card details, or other personal information, by posing as a trustworthy entity. This is typically done through deceptive emails, text messages, or fake websites that mimic legitimate organizations, such as banks, social media platforms, or online retailers.

Malware: Malware, short for malicious software, is a type of software that is designed to harm, exploit, or gain unauthorized access to digital devices or networks. Examples of malware include viruses, worms, Trojans, and spyware. Malware can be installed on a device without the user's consent and can steal information, disrupt operations, or cause damage to the device or network.

Ransomware: Ransomware is a type of malware that encrypts data on a victim's device and demands a ransom in exchange for the decryption key. This can prevent individuals or organizations from accessing their own data until the ransom is paid. Ransomware attacks can result in financial losses, data breaches, and operational disruptions.

Social Engineering: Social engineering is a technique used by cyber attackers to manipulate individuals into revealing sensitive information or performing actions that compromise security. This can include tactics such as pretexting, where attackers create a fake scenario to gain trust, or baiting, where they entice individuals with a reward or incentive to divulge information.

These are just a few examples of common cyber threats, and it's important to stay vigilant and take preventive measures, such as being cautious of suspicious emails or links, keeping software and devices up-to-date, and practicing safe online behaviors, to protect against these threats.

5. How Cyber Threats Compromise Personal Information and Cause Harm

Cyber threats, such as phishing, malware, ransomware, and social engineering, can compromise personal information and cause significant harm to individuals and organizations. Let's take a closer look at how these threats can compromise personal information and cause harm:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, June 2023

Phishing: Phishing attacks can trick individuals into revealing their usernames, passwords, credit card details, and other sensitive information to cyber attackers. This information can be used to gain unauthorized access to personal accounts, steal money, or commit identity theft. Phishing attacks can also lead to reputational damage, financial loss, and emotional distress.

Malware: Malware can be designed to steal personal information, such as usernames, passwords, financial data, or personal documents, from infected devices. This information can be used for identity theft, financial fraud, or other malicious activities. Malware can also disrupt operations, damage files or systems, and result in financial losses or legal liabilities.

Ransomware: Ransomware attacks can encrypt personal data on a victim's device and demand a ransom for the decryption key. If the ransom is not paid, victims may lose access to their important files or data, leading to financial losses, operational disruptions, and reputational damage.

Social Engineering: Social engineering attacks can manipulate individuals into revealing personal information or performing actions that compromise security. For example, pretexting attacks may trick individuals into divulging personal information by creating a fake scenario or pretext. Baiting attacks may entice individuals with a reward or incentive to disclose sensitive information. These attacks can result in unauthorized access to personal accounts, identity theft, financial fraud, and other harmful consequences.

It's important to be aware of how cyber threats can compromise personal information and cause harm, and take proactive measures to protect against them, such as being cautious online, keeping software and devices up-to-date, using strong and unique passwords, and being vigilant against social engineering tactics.

6. Importance of Strong and Unique Passwords for Online Accounts

Passwords are a critical aspect of online security, as they serve as a key to unlock access to various online accounts. Using strong and unique passwords is essential to protect personal information and prevent unauthorized access. Here's why:

Prevents Password Guessing: Weak passwords, such as "123456" or "password," are easily guessable by cyber attackers using automated tools. Strong and unique passwords that include a combination of uppercase and lowercase letters, numbers, and special characters make it much harder for attackers to guess or crack passwords, increasing the security of online accounts.

Protects Against Brute Force Attacks: Brute force attacks are automated attempts to crack passwords by systematically trying every possible combination until the correct password is found. Strong and unique passwords with a sufficient length and complexity make it computationally infeasible for attackers to crack passwords using brute force attacks.

Guards Against Credential Stuffing: Credential stuffing is a type of attack where attackers use stolen usernames and passwords from one account to gain unauthorized access to other accounts where the same credentials are used. Using unique passwords for each online account minimizes the risk of credential stuffing attacks, as attackers won't be able to use the same password across multiple accounts.

Enhances Overall Account Security: Using strong and unique passwords adds an extra layer of protection to online accounts, reducing the risk of unauthorized access, data breaches, and identity theft. It helps safeguard personal information, financial data, and other sensitive data stored in online accounts, protecting individuals from potential financial losses, reputational damage, and legal liabilities.

Provides Peace of Mind: Using strong and unique passwords for all online accounts gives individuals peace of mind knowing that they have taken a proactive step to protect their personal information and online accounts from cyber threats. It's a simple but effective measure that can greatly enhance overall online security.

It's crucial to emphasize the importance of using strong and unique passwords for all online accounts and encourage students to create and maintain strong passwords to protect their online presence and personal information. Additionally, it's important to educate them on the proper way to store and manage passwords securely, such as using password managers, avoiding sharing passwords with others, and regularly updating passwords.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, June 2023

7. Tips for Creating Strong Passwords and Avoiding Common Password Mistakes

Creating strong and unique passwords is essential for online security. Here are some tips for creating strong passwords and avoiding common password mistakes:

- Length and Complexity: Use passwords that are at least 12 characters long and include a combination of uppercase and lowercase letters, numbers, and special characters. Avoid using easily guessable information like names, birthdates, or common words.
- Avoid Common Patterns: Avoid using common patterns or sequences like "12345" or "qwerty" as they are easily guessable. Use random combinations of characters that are not easily predictable.
- Don't Use Personal Information: Avoid using personal information like names, addresses, phone numbers, or other easily obtainable information as part of your password. This information can be easily guessed or obtained through social engineering attacks.
- Unique Passwords: Use unique passwords for each online account to prevent credential stuffing attacks. Avoid using the same password across multiple accounts as it increases the risk of unauthorized access if one account is compromised.
- Regularly Update Passwords: Regularly update passwords for all online accounts, ideally every 3-6 months or sooner if there is any suspicion of a security breach. Avoid reusing old passwords or using similar passwords for multiple accounts.
- Use Password Managers: Consider using a password manager tool to generate and store complex passwords securely. Password managers can help you manage and remember strong and unique passwords for each online account without the need to memorize them all.
- Be Cautious with Password Recovery Questions: Avoid using easily guessable answers for password recovery questions, such as your pet's name, mother's maiden name, or favorite sports team. Use unique answers that are not easily obtainable from public information.
- Keep Passwords Confidential: Never share passwords with anyone, including friends, family, or even trusted individuals. Keep your passwords confidential to prevent unauthorized access to your accounts.

By following these tips, students can create strong and unique passwords for their online accounts, minimizing the risk of unauthorized access, data breaches, and identity theft. It's important to emphasize the significance of password security and encourage responsible password management practices among students to protect their personal information online.

8. Risks of Sharing Personal Information on Social Media Platforms

Social media platforms are widely used for communication, sharing photos and personal updates, and connecting with others. However, sharing personal information on social media platforms can also pose risks to online security and privacy. Here are some risks to be aware of:

- Privacy Risks: Social media platforms often have privacy settings that allow users to control what information is visible to others. However, many users may not configure these settings properly, inadvertently sharing personal information with a wider audience than intended. This can lead to privacy breaches and expose personal information to strangers, cyber attackers, or identity thieves.
- Identity Theft: Cyber criminals may use personal information shared on social media platforms to steal identities and commit identity theft. Information such as full name, birthdate, location, phone number, and email address can be used to create fake accounts, conduct phishing attacks, or commit other types of fraud.
- Social Engineering Attacks: Cyber attackers may use the personal information shared on social media platforms to conduct social engineering attacks. By gathering personal details about an individual, such as their hobbies, interests, and relationships, attackers can craft convincing messages or emails to manipulate the individual into revealing sensitive information or clicking on malicious links.
- Location Tracking: Many social media platforms allow users to "check-in" or share their location. This can reveal an individual's whereabouts and routines, posing risks such as stalking, physical harm, or theft.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, June 2023

- Reputation Risks: Sharing personal information on social media platforms can impact an individual's reputation. Inappropriate or compromising posts, photos, or comments can have negative consequences on personal and professional relationships, job prospects, and future opportunities.
- Social Risks: Sharing personal information on social media platforms can also expose individuals to social risks such as cyberbullying, harassment, or unwanted contact from strangers. It's important to be cautious about the information shared online and avoid disclosing sensitive or personal details.
- Data Collection and Tracking: Social media platforms often collect and track user data for various purposes, including targeted advertising. This can result in personal information being used for commercial purposes without the user's consent, and can also increase the risk of data breaches or unauthorized access to user data.

It's crucial to educate students about the risks associated with sharing personal information on social media platforms and emphasize the importance of being cautious and responsible while using social media. Encourage them to review and adjust their privacy settings, think twice before sharing personal information, and be mindful of the potential consequences of their online actions

9. Tips for Safeguarding Personal Information Online

Safeguarding personal information online is crucial to protect against cyber threats. Here are some tips to help students safeguard their personal information online:

Be cautious with online forms: Avoid providing personal information, such as full name, address, phone number, or email address, on unfamiliar or suspicious online forms, websites, or pop-up windows. Always verify the legitimacy of the website or form before providing any personal information.

- Review privacy settings: Review and configure privacy settings on social media platforms, online accounts, and devices to ensure that personal information is not shared with a wider audience than intended. Limit the amount of personal information that is visible to others and avoid sharing sensitive information publicly.
- Use strong and unique passwords: Use strong, unique, and complex passwords for all online accounts. Avoid using easily guessable passwords, such as "password123" or "123456", and consider using a passphrase or password manager to help generate and store strong passwords securely.
- Avoid oversharing: Be mindful of the information shared online, including personal details, photos, locations, and activities. Avoid oversharing personal information on social media platforms, public forums, or other online platforms, as this can increase the risk of identity theft, social engineering attacks, and other cyber threats.
- Be cautious with email attachments and links: Be cautious when opening email attachments or clicking on links, especially if they are from unknown or suspicious sources. These can contain malware or phishing attempts that can compromise personal information and lead to cyber attacks.
- Keep software and devices updated: Regularly update all software, applications, and devices with the latest security patches and updates. This helps to fix known vulnerabilities and protect against cyber attacks that exploit security weaknesses.
- Be cautious with online friends and strangers: Be cautious with online friendships and interactions, and avoid sharing personal information with strangers online. Be aware of the risks of cyberbullying, online harassment, and other online threats, and report any suspicious or threatening behavior to a trusted adult or authority.

By following these tips, students can take proactive measures to safeguard their personal information online and reduce the risks of cyber threats. Encourage them to be cautious, responsible, and vigilant when sharing personal information online, and to prioritize their online privacy and security.

10. General Tips for Safe Internet Practices

Safe internet practices are essential to protect against cyber threats. Here are some general tips for safe internet practices that students should keep in mind:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, June 2023

- Be cautious when clicking on links: Avoid clicking on suspicious or unfamiliar links, especially in emails, text messages, or social media messages. Verify the legitimacy of the link before clicking on it, and hover over the link to check the URL before clicking.
- Be careful with email attachments: Be cautious when downloading and opening email attachments, especially if they are from unknown or suspicious sources. Malware and viruses can be hidden in attachments, which can compromise the security of the device and personal information.
- Avoid visiting unfamiliar websites: Be cautious when visiting unfamiliar websites, especially those that ask for personal information or financial details. Stick to trusted websites and avoid clicking on ads or links that seem suspicious or untrustworthy.
- Practice safe social media habits: Be mindful of the information shared on social media platforms, including personal details, photos, locations, and activities. Adjust privacy settings to limit the visibility of personal information, and be cautious when accepting friend requests or interacting with strangers online.
- Keep software and devices updated: Regularly update all software, applications, and devices with the latest security patches and updates. This helps to fix known vulnerabilities and protect against cyber attacks that exploit security weaknesses.
- Use trusted sources for downloads: Download software, applications, and files only from trusted sources, such as official websites or app stores. Avoid downloading files from unfamiliar websites or peer-to-peer networks, as they may contain malware or viruses.
- Use public Wi-Fi with caution: Avoid using public Wi-Fi networks for sensitive activities, such as online banking or accessing personal information. Public Wi-Fi networks may not be secure, and cyber criminals can intercept data transmitted over these networks.
- Be cautious with online gaming: Be cautious when engaging in online gaming and avoid sharing personal information or accepting friend requests from strangers. Use privacy settings and limit the amount of personal information shared in gaming profiles.

These general tips for safe internet practices can help students develop safe online habits and protect themselves from common cyber threats. Encourage them to be vigilant, cautious, and responsible when using the internet, and to report any suspicious activities or incidents to a trusted adult or authority

11. Be Critical and Vigilant While Using the Internet

In today's digital world, it's crucial to be critical and vigilant while using the internet. Cyber threats are constantly evolving, and it's important to stay alert and cautious. Here are some key points to emphasize:

- Think before you click: Don't click on links or download attachments without verifying their legitimacy. Be cautious of suspicious or unfamiliar links, especially in emails, text messages, or social media messages. Think critically and evaluate the source and content before clicking.
- Verify information: Not all information on the internet is accurate or trustworthy. Encourage students to verify information from multiple reliable sources before accepting it as true. Teach them to be critical thinkers and fact-checkers to avoid falling for misinformation or fake news.
- Be cautious with personal information: Remind students to be cautious when sharing personal information online, including on social media platforms, online forms, or websites. Encourage them to limit the amount of personal information shared and adjust privacy settings to protect their privacy.
- Keep passwords secure: Emphasize the importance of using strong and unique passwords for all online accounts and the risks of password reuse. Encourage students to avoid common password mistakes, such as using easily guessable information or using the same password for multiple accounts are from unknown or suspicious sources. Malware and viruses can be hidden in attachments, which can compromise the security of the device and personal information.
- Report suspicious activities: Encourage students to report any suspicious activities or incidents to a trusted adult or authority, such as a teacher, parent, or school administrator. Reporting suspicious activities can help prevent potential cyber threats and protect others.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, June 2023

- Stay updated with security measures: Teach students about the importance of keeping their devices, software, and applications updated with the latest security patches and updates. Remind them to enable security features, such as firewalls and antivirus software, to add an additional layer of protection.

Being critical and vigilant while using the internet is crucial in today's digital landscape. By developing these skills, students can protect themselves from cyber threats, make informed decisions, and use the internet safely and responsibly.

12. Cyber Bullying and Its Impact

Cyber bullying is a form of bullying that occurs online, typically through social media platforms, chat rooms, or other digital communication channels. It can have serious and lasting impacts on individuals, and it's important to raise awareness about this issue. Here are some key points to discuss:

- Definition of cyber bullying: Explain that cyber bullying involves using technology, such as smartphones, computers, or tablets, to harass, intimidate, or harm others online. It can take various forms, including sending threatening messages, spreading rumors, sharing embarrassing photos or videos, or creating fake profiles to impersonate others.
- Impact on individuals: Discuss the emotional, psychological, and social impact of cyber bullying on individuals. It can cause stress, anxiety, depression, and low self-esteem. Victims of cyber bullying may experience social isolation, loss of self-confidence, academic decline, and even physical health issues. It can have serious and lasting impacts on the mental and emotional well-being of individuals.
- Legal and ethical implications: Emphasize that cyber bullying is not only harmful but also illegal in many jurisdictions. Discuss the legal consequences and potential legal actions that can be taken against cyber bullies, including criminal charges, civil lawsuits, and school or workplace disciplinary actions. It's important to understand the ethical implications of cyber bullying and the responsibility we have to treat others with respect and kindness online.
- Prevention and intervention: Discuss the importance of prevention and intervention strategies to address cyber bullying. Encourage students to speak up and report any instances of cyber bullying they witness or experience. Discuss the role of trusted adults, such as teachers, parents, or school administrators, in providing support and guidance to victims of cyber bullying. It's important to create a safe and inclusive online environment where everyone can thrive without fear of bullying.
- Responsible online behavior: Empha-size the importance of responsible online behavior, including treating others with kindness, respecting their privacy, and using technology in a positive and responsible manner. Discuss the concept of digital citizenship and the need to be good online citizens by being respectful, empathetic, and responsible in our online interactions.

Cyber bullying can have serious and damaging impacts on individuals. It's crucial to raise awareness about this issue and promote responsible online behavior to prevent cyber bullying and provide support to victims.

13. Recognizing and Responding to Cyber Bullying

It's important for students to know how to recognize and respond to cyber bullying if they encounter it online. Here are some key points to discuss:

- Recognizing cyber bullying: Provide examples of different types of cyber bullying, such as sending hurtful mes-sages, spreading rumors, sharing embarrassing photos or videos, or creating fake profiles to impersonate others. Explain that cyber bullying can happen through various online platforms, including social media, messaging apps, and online forums.
- Responding to cyber bullying: Discuss the appropriate ways to respond if students witness or experience cyber
- bullying. Encourage them to not re-spond to cyber bullies or retaliate, as it can escalate the situation. Instead, advise them to save evidence of the cyber bullying, such as screenshots or copies of messages, and report it to a trusted adult or authority figure, such as a teacher, parent, or school administrator.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, June 2023

- Reporting cyber bullying: Explain the importance of reporting cyber bullying incidents to trusted adults or authorities. Discuss the reporting mechanisms available on various online platforms, such as "report" or "block" options, and how to use them. Encourage students to keep the lines of communication open with trusted adults and seek support if they are being cyber bullied.
- Seeking help and support: Discuss the importance of seeking help and support if students experience cyber bullying. Encourage them to talk to a trusted adult, such as a teacher, parent, or school counselor, about what they are going through. Remind students that they are not alone

Recognizing and responding to cyber bullying is crucial in creating a safe and inclusive online environment. Encourage students to take action and seek help if they encounter cyber bullying, and emphasize the importance of responsible and respectful online behavior.

III. CONCLUSION

Cybersecurity awareness plays a vital role in the protection of digital assets and the prevention of cyber threats. With the increasing sophistication and frequency of cyber attacks, it is imperative that individuals, organizations, and society as a whole prioritize cybersecurity awareness as an essential component of their digital lives. cybersecurity awareness is a shared responsibility that requires continuous education, vigilance, and proactive measures. By embracing a holistic approach that integrates individual, organizational, and societal dimensions, we can create a culture of cybersecurity awareness that empowers indi-viduals, fortifies organizations, and builds resilient digital communities.As the digital landscape continues to evolve, it is essential that we remain committed to enhancing cybersecurity awareness. By doing so, we can mitigate cyber risks, protect our digital assets, and ensure a safer and more secure digital future for all

REFERENCES

[1] G. V Cormack, “Email Spam Filtering: A Syste-matic Review,” Foundations and Trends® in Information Retrieval, vol. 1, 2008.
[2] K. Bissell, R. la Salle, and C. P. Dal, “)e 2020 Cyber Security Report,” 2020, https://pages.checkpoint.com/cybersecurityreport-2020.
[3] Mimecast, “Email Security Risk Assessment: Quarterly Report,” 30 pages, 2019, https://www.mimecast.com/globalassets/documents/whitepapers/esrawhite-paper-june2019.pdf.
[4] Positive Technologies, “Cybersecurity)reatscape Q4,” 2018, https://www.ptsecurity.com/ww-en/analytics/cybersecuritythreatscape-2018-q4/.
[5] M. Lee, “Phishing Scams Cost American Busi-nesses Half A Billion Dollars A Year,” 2017, https://www.forbes.com/sites/leemthews/%202017/05/05/phishing-scams-cost-americanbusinesses-half-a-billion-ollars-ayear/#bdec44b3fa1c.
[6]https://www.jiit.ac.in/sites/deault/files/Cyber%20Security%20Awareness%20Hand%20Book.pdf
[7] Khalid, F., Daud, M. Y., Rahman, M. J. A., & Nasir, M. K. M. (2018). An investigation of university students’ awareness on cyber security. International Journal of Engineering & Technology, 7(421), 11-14.
[8] Carstens, D., Sater, M. C.-B., Pamela, R., et al. (2004). Evaluation of the human impact of password authentication practices on information securi-ty. Informing Science, 7, 67–85. http://s.dic.cool/S/qeUrlL1R. Accessed 20 July 2021.
[9] Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. The African Journal of Information and Communication, 20, 133–155. https://doi.org/10.23962/10539/23572