Grenze International Journal of Engineering and Technology, June Issue

Cyber Hygiene in Higher Educational Institutes

Shalabh Agarwal[1] and Anweshan Mukherjee[2]
[1-2]Department of Computer Science, St. Xavier's College, Kolkata, India
Email: shalabh@sxccal.edu, anweshanmukherjee22@gmail.com

***Abstract*— Internet has become one of the integral parts of our daily life. It has transformed the way we communicate; make friends, share updates, play games, and shop. They are impacting most aspects of our day-to-day life. Education is one of the important sectors for dissemination of information on prevention of cyber-crimes and reiterated that students can act, as a force multiplier to create an ecosystem for cyber security and to prevent cyber-crimes. Cyberspace connects us virtually with crores of online users across the globe. With increasing use of cyberspace, cybercrimes especially against women and children such as cyber stalking, cyber bullying, cyber harassment, child pornography, rape content, etc. are also increasing rapidly. To stay safe in the online world, it is important to follow some cyber safe practices which may help in making our online experience more productive. Cyber Hygiene is the need-of-the-hour in the world which is rapidly transforming to an online mode. This paper focuses on how cyber hygiene can be introduced and implemented in higher educational institutes so that both direct and indirect stakeholders of the institute are safe from security threats.**

***Index Terms*— Cyber Hygiene, Cyber Threats, Cyber Security, Browsing and Password.**

I. INTRODUCTION

In this world where almost everything is shifting to an online mode, cyber hygiene is of utmost importance. The Covid pandemic has made us realize the wonders we can do by shifting to the online mode or at least by transforming some of the work to an online platform thus operating a hybrid platform. But these advantages bring in some cons as well. According to Internet Organized Crime Threat Assessment (IOCTA), there has been an increase in the number of cyber-crimes happening since the lockdown started in various countries. [1][2] Phishing, social engineering, ransomware attacks, online scams and other types of attacks have become more frequent as more people shifted to the digital world. Thus, the need for cyber hygiene arises.

In Higher Educational Institutes, incorporating proper security mechanisms and educating people about digital crimes are crucial because it contains sensitive information of students, professors, staff, and others like banking information, graduation marks, and other types of records. The policies governing them should be updated regularly such that the procedures that enable cyber hygiene to be implemented are financially feasible. [5]

In simplest terms, the definition of cyber hygiene means taking care of your digital self just like you would your physical self. Just as you would not leave your house unlocked or your car running with the keys in the ignition, you should not neglect basic security measures for your online accounts and devices. It refers to a set of practices and behaviors that individuals and organizations should follow to maintain good cybersecurity and protect their digital assets, systems, and data from cyber threats. These practices are akin to personal hygiene in the physical world, where regular washing and cleanliness help prevent illness and maintain health. In the digital realm, cyber

Grenze ID: 01.GIJET.10.2.506

hygiene helps prevent cyberattacks and maintain the health and security of digital environments.
Cyber hygiene is crucial for safeguarding digital assets, ensuring data privacy, and protecting against a wide range of cyber threats. It is essential for individuals, organizations, and even governments to prioritize and practice good cyber hygiene to maintain security, privacy, and trust in the digital world.

II. Types Of Cyber Threats In Higher Educational Institutes (HEI)

A. Ransomware Attack

Malware called ransomware is made to prevent the administrator or the stakeholders of the institute from accessing files on their server or any computer on the network. This puts the educational institute in a situation where paying the ransom and requesting for the decryption key or method is the quickest and least expensive method to recover their data. If they fail to pay the ransom amount, the stakeholders are at risk of getting their confidential data compromised and leaked.
As the educational sector started transforming to an online mode during the pandemic, the number of ransomware attacks on educational institutes surged rapidly throughout the world. The networks were most vulnerable during the testing phase when the institutes were gradually adapting to have sensitive data on the cloud such as during online admission process.

B. Phishing Attack

There can be several emails sent to the administrator trying to manipulate that person into believing that the source is a trusted one and ultimately get the institute's data compromised. It is a kind of social engineering attack where attackers try to play with human psychology and get hold of sensitive data.

C. Outdated System

It is quite often that educational institutes suffer cyber-attacks due to a vulnerability mainly created due to presence of outdated system. The attackers try by all possible means to attack a system and if the system's security system is not up-to-date, data compromise is highly probable.

D. Intra-network Attack

In smart campuses, where there are multiple Internet of Things (IoT) devices such as smart lights connected over the Internet, if the network gets compromised, the usual environment inside the campus gets disturbed.

E. Virus

There may be instances when students copy their classwork into their pen drives after the lecture is done. Those pen drives may be virus infected, thus degrading the system.

F. Drive-by-download Attack

There may be college staff or students browsing the Internet and they accessed a website which automatically started the download of some malicious code thus compromising the system.

G. Denial-of-Service Attack

Attackers can target the network and server of the institute and block legitimate users from accessing the data during the time when the website gets most hits, such as during publication of semester results or online admission system.

H. SQL Injection

Most of the educational institutes have a query text box on their website. Users type in the type of queries to search for in the database. Attackers can use this and place malicious queries in that query text box to gain access to confidential information.

I. Domain Spoofing

People can register their own websites with the domain very close to the actual domain of the institute. Users may get confused and access their website and thus may enter their sensitive data there or just form a barrier to gain access to the original website.

J. Indirect Attack Through Plugins

Most educational institutes use plugins of some payment gateway for enabling online payment. If that payment gateway somehow gets compromised, the payment system for that educational institute also suffers leading to loss of availability.

III. Cyber Hygiene Awareness Within Higher Educational Institutes (HEI)

There have been multiple research surveys done to check how aware users are of cyber hygiene. [3] Among them, a survey consisted of questioning 329 homes on their compliance with digital security mechanisms such as firewalls, intrusion detection systems, antivirus and other processes for ensuring secure computing. Fig. 1 shows some of the results obtained from this survey.

Ovelgönne at al. [4] conducted research survey to understand that software developers faced the most malware attacks; gamers and computer professionals followed them. Dawson et al. [6] conducted a survey on cyber-attacks and found out that weak passwords which can be cracked easily are a major reason for network vulnerability. Thus, having a strong authentication mechanism in place is important for maintaining cyber hygiene. Users tend to reuse passwords for multiple sites or share with others which are critical.

Caputo et al. [6] as a method of implementing cyber hygiene, trained an organization's employees not to respond to suspicious emails. Markelj et al. [7] inspected the perception of cyber hygiene among mobile phone users. Table I shows the data found by them.

Ugwu et al. [8] described the association of demographics, age and level of education with the cyber hygiene culture namely, storage and virus attack, social network, authentication and social engineering. Their study was dependent on a questionnaire used to extract insights on demographics, users' internet activities including the devices used, users' knowledge on security threats and the level to which culture of cyber-hygiene was prevalent. The parameters derived from the questionnaire were total cyber hygiene culture, categorized average total cyber hygiene culture, total knowledge of concept, average total knowledge of concept and categorized average total knowledge of concept. These were derived in accordance with various statistical measures such as Chi-Square test.

Ponemon Institute published a report [3] stating that American organizations face the biggest problem due to cyber-attacks. Fig. 2 shows the percentages of various types of attacks.

In January, 2023, we conducted a survey at our college, which is a HEI of repute in India approximately having 400 teachers and 8000 students, to understand the awareness about cyber hygiene amongst the students and staff and the results are as shown in Table II.

Using the charts as displayed in Table II, we may conclude the awareness as given in Table III.

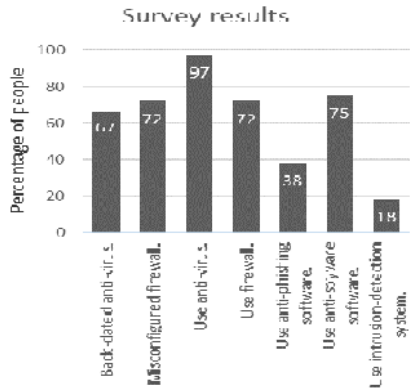


Figure 1. Results of survey on cyber hygiene.

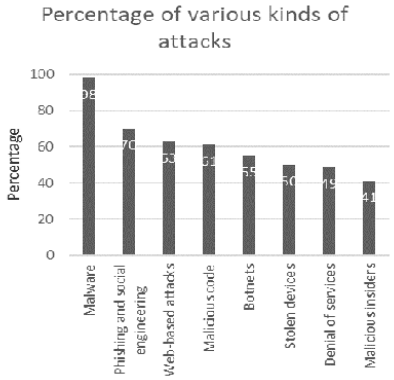


Figure 2. Results of survey on various kinds of attacks on US organizations.

TABLE I. RESULTS FOUND ON QUESTIONING MOBILE PHONE USERS

Percentage of people	Activity
39.1%	Aware of malware threat.
39.7%	Aware of spyware threat.
45.3%	Aware of rootkit threat.

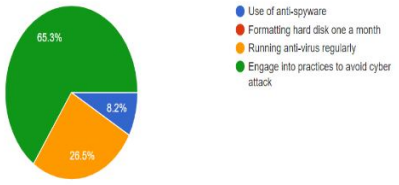
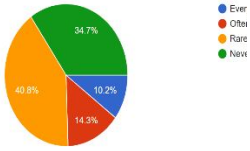
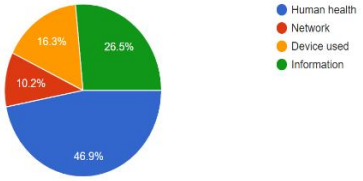
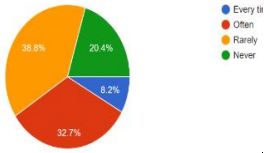
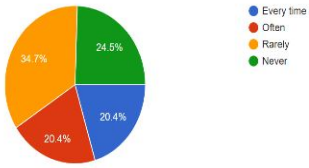
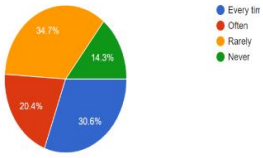
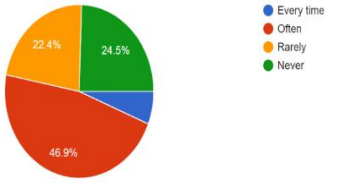
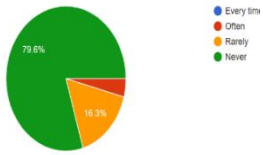
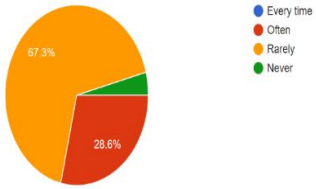
TABLE III. ANALYSIS OF SURVEY CONDUCTED IN COLLEGE

Topic	Level
Understanding of cyber hygiene	Moderate
Use of protection tools and software	Poor

56.8%	Did not have authentication mechanism in place.
40%	Aware of remote data removal in case of mobile phone theft but that option was disabled.

Effective use of passwords	Poor
Disclosure of identity	Moderate

TABLE II. RESULTS OF SURVEY CONDUCTED IN COLLEGE

Question	Results	Question	Results
What is cyber hygiene?		When do you use anti-phishing software?	
Poor cyber hygiene affects:		How often do you type a link on the address bar rather than just clicking on it?	
When do you use anti-spyware?		How often do you use any of your real name, email address and date of birth on social media?	
How often do you use a single password for multiple accounts?		How often do your respond to emails or links that are asking for sensitive information?	
How often do you change your passwords?			

A lack of Cyber Hygiene increases the risk of a cyber-attack. According to Stealth Labs, education was one of the most vulnerable sectors for cyber-attack, making up almost 64% of all malware attacks, proving that there is a

need for improved cyber-hygiene in education. Thirty percent of users in education were victims of phishing, a kind of cyber-attack where cyber-criminals pose as reputable companies to steal information such as usernames and passwords. (StealthLabs).

“The sudden shift to remote learning triggered by the pandemic has further deteriorated the situation. With students increasingly using their personal computers and unsecured networks to join online classes, the threat vector of the education sector is proliferating.” (StealthLabs)

If a student is not aware of basic cyber-hygiene and connects to an unsecure network, shares their password or username, or does not verify people’s identities, they could become victim to a multitude of cyber-attacks.

Cyber hygiene awareness is a critical component of promoting good cybersecurity practices among individuals, organizations, and communities. It involves educating people about the importance of cyber hygiene and providing them with the knowledge and skills needed to protect themselves and their digital assets from cyber threats. Some key aspects of cyber hygiene awareness are as follows:

A. Education and Training

Raise awareness through educational programs and training sessions that teach individuals and employees about the basics of cyber hygiene, including password management, recognizing phishing emails, and updating software.

B. Communication

Use various communication channels to disseminate information about cyber hygiene, such as emails, newsletters, websites, social media, and posters. Make sure that the information is clear, concise, and accessible.

C. Cybersecurity Policies

Ensure that organizations have clear cybersecurity policies in place and that employees are aware of these policies. Regularly communicate updates and reminders about policy compliance.

D. Cybersecurity Awareness Campaigns

Launch awareness campaigns that focus on specific cybersecurity topics or themes. These campaigns can use creative and engaging content to capture the audience's attention and reinforce key messages.

E. Simulated Phishing Exercises

Conduct simulated phishing exercises within organizations to test employees' ability to identify phishing emails. Provide immediate feedback and additional training to those who fall for the simulations.

F. Access to Resources

Make cybersecurity resources, such as online courses, articles, and guides, readily available to students, teachers and employees so they can continually educate themselves about cyber threats and best practices.

G. Community Engagement

Extend cyber hygiene awareness efforts to the broader community by participating in local cybersecurity initiatives, hosting workshops, and collaborating with educational institutions.

H. Customized Messaging

Tailor cyber hygiene awareness messages to different audiences, such as employees, students, teachers and alumni/ae. Recognize that different groups may have varying levels of cybersecurity knowledge and concerns.

I. Leadership Involvement

Encourage leadership within the instituion to spread cybersecurity awareness and set an example by practicing good cyber hygiene themselves.

J. Collaboration

Foster collaboration between government agencies, industry organizations, and cybersecurity experts to create a unified front in promoting cyber hygiene awareness and best practices within the institution and stakeholders.

Cyber hygiene awareness is an ongoing effort that requires commitment and persistence. By fostering a culture of cybersecurity awareness and empowering individuals and organizations with the knowledge and tools to protect themselves, we can collectively reduce the risk of falling victim to cyberattacks and enhance overall cybersecurity posture.

IV. Cyber Hygiene Best Practices In Higher Educational Institutes

After considerable research on the implementation of cyber hygiene in HEIs, we propose five key areas which need to be addressed in details and wide awareness campaigns cutting across all the stakeholders must be carried out regularly. The five key areas are as mentioned in Fig. 3.

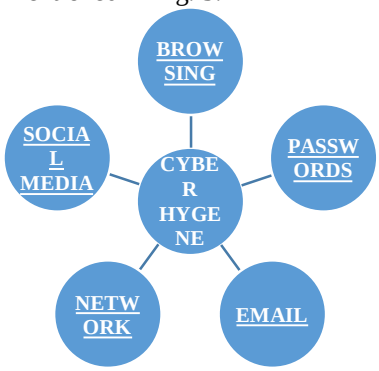


Figure 3. Five key areas of cyber hygiene

A. Browsing

Browsing best practices are guidelines and recommendations that individuals should follow to enhance their online security and privacy while using web browsers. Web browsers are one of the primary gateways to the internet, and securing them is crucial to protect personal information and prevent cyberattacks. Mentioned below are some important browsing best practices:

- *Keep your browser updated*: Regularly update your web browser to the latest version. Browser updates often include security patches to address vulnerabilities.
- *Enable automatic updates*: Set your browser to automatically download and install updates. This ensures you are always running the most secure version.
- *Use a secure and up-to-date browser*: Choose a reputable browser known for its security features and frequent updates.
- *Install browser extensions with caution:* Be cautious when installing browser extensions and add-ons. Only install those from trusted sources, and review permissions they request.
- *Enable multi-factor authentication (MFA):* If your browser supports MFA for account access, enable it to add an extra layer of security.
- *Review browser settings:* Regularly review your browser's privacy and security settings to ensure they are configured to your desired level of protection. This includes settings related to cookies, tracking, and pop-ups.
- *Clear cookies and cache*: Periodically clear your browser's cookies and cache to remove stored data that can be used to track your online activities.
- *Use https*: Whenever possible, visit websites that use https (secure browsing). Modern browsers often display a padlock icon to indicate a secure connection.
- *Be cautious with downloads*: Be cautious when downloading files from the Internet. Only download files from reputable sources, and regularly scan downloaded files for malware.
- *Use a VPN (Virtual Private Network):* Consider using a VPN to encrypt your internet connection and protect your online privacy, especially when using public Wi-Fi networks.
- *Beware of phishing attacks*: Be watchful of unsolicited emails, messages, or pop-ups asking for personal or financial information. Verify the legitimacy of websites and requests.
- *Regularly check for updates and security patches*: Keep your operating system and all software, including browser plugins and extensions, up-to-date with the latest security patches.
- *Log out of accounts*: Always log out of your accounts, especially on public or shared computers.
- *Educate yourself about phishing and scams:* Stay informed about common online scams and phishing techniques. Knowing what to look for can help you avoid falling victim to cybercriminals.
- *Regularly back up your data:* Back up important data regularly to ensure you can recover it in case of a cyber incident.

- *Consider browser privacy plugins and settings*: Explore various browser privacy plugins or settings that block trackers, ads, and unwanted scripts to enhance your online privacy.
- *Be cautious with autofill and saved passwords*: Use autofill and saved passwords sparingly and only on trusted devices. Be cautious when prompted to save passwords on public computers.
- *Read browser security updates and advisories*: Stay informed about security updates and advisories released by your browser provider. They may provide important information about known vulnerabilities and fixes.
- *Secure Social Media Practices:* Be cautious about the information you share on social media platforms. Cybercriminals can use this information to craft convincing attacks.

B. Passwords

Password security is crucial for protecting your online accounts and sensitive information. Cybercriminals often target weak or easily guessable passwords to gain unauthorized access. By following these password best practices, you can significantly enhance your online security and reduce the risk of falling victim to cyberattacks. Strong, unique passwords are a fundamental aspect of online safety. Here are some password best practices to help you create strong, secure passwords:

- *Use Complex Passwords*: Create passwords that are at least 12-16 characters long and include a mix of uppercase and lowercase letters, numbers, and special characters (e.g., !, @, #, $, %).
- *Avoid Easily Guessable Information*: Avoid using easily guessable information like common words, phrases, birthdays, and names. Also, refrain from using consecutive or repetitive characters (e.g., "12345" or "aaaaa").
- *Unique Passwords for Each Account*: Use a unique password for each of your online accounts. Reusing passwords across multiple accounts increases your vulnerability if one account is compromised.
- *Consider Passphrases*: Passphrases are longer, easier-to-remember sequences of words or phrases. For example, "Honesty@is@the@best@policy#2022" is a strong passphrase.
- *Use a Password Manager*: Consider using a reputable password manager to generate, store, and autofill complex passwords. Password managers help you maintain unique and strong passwords for each account.
- *Change Default Passwords*: If you have any devices or accounts with default passwords, change them immediately. Default passwords are easy targets for attackers.
- *Enable Multi-Factor Authentication (MFA):* Whenever possible, enable MFA for your online accounts. MFA adds an extra layer of security by requiring an additional verification step, such as a one-time code sent to your mobile device.
- *Regularly Update Passwords:* Change passwords periodically, especially for critical accounts like email, banking, and social media. Consider changing them every 3-6 months.
- *Beware of Phishing:* Be cautious of phishing emails or websites that impersonate legitimate services and ask for your password. Always verify the authenticity of the site before entering your credentials.
- *Avoid Using Personal Information:* Avoid using easily obtainable personal information, such as your name, username, or the names of family members, in your passwords.
- *Randomize Passwords:* Avoid using easily guessable patterns like "123456" or "password." Use randomly generated characters for better security.
- *Test Your Passwords:* Some websites and tools offer password strength meters that can help you gauge the security of your chosen passwords. Take advantage of these tools.
- *Secure Your Password Reset Process:* Ensure that the process for resetting passwords is secure and not easily exploited by attackers.
- *Keep Passwords Private:* Do not share your passwords with anyone, and avoid writing them down in easily accessible places.

C. Email

Email is a critical communication tool, but it's also a common target for cyberattacks and phishing attempts. Implementing best practices for email usage can help you protect your personal information, reduce the risk of security breaches, and maintain a secure online presence. By following these email best practices, you can reduce the risk of falling victim to email-based cyberattacks, protect your personal information, and maintain a more secure email communication environment. Following are some email best practices:

- *Beware of Phishing Emails*: Be cautious when opening emails from unknown or suspicious senders. Avoid clicking on links or downloading attachments from unsolicited emails.

- *Verify Sender Identities:* Before responding to any email requesting personal or financial information, verify the sender's identity and confirm that the email is legitimate. Contact the sender through a trusted channel if in doubt.
- *Use Secure Email Services:* Choose reputable email service providers that offer strong security features, including encryption in transit and at rest. Look for "https://" when accessing your email account online.
- *Be Wary of Urgent Requests*: Keep away from emails that pressure you to act urgently or provide personal information quickly. Take your time to verify the request.
- *Protect Personal and Financial Information*: Avoid sending sensitive personal or financial information via email. Use secure methods or encrypted messaging services for such communication.
- *Use Email Filters*: Enable spam filters and email scanning services to automatically filter out suspicious or malicious emails.
- *Regularly Update Software*: Keep your email client, browser, and operating system up-to-date with the latest security patches and updates.
- *Use Encrypted Email Services:* Consider using end-to-end encrypted email services for sensitive communications to protect the content of your messages.
- *Regularly Review Email Settings:* Periodically review and update your email account settings, including password recovery options, forwarding rules, and security preferences.
- *Be Cautious with Email Forwarding and Reply-All:* Be careful when forwarding emails or replying to messages with multiple recipients. Avoid disclosing sensitive information to unintended recipients.
- *Secure Your Contacts:* Be cautious about sharing your contacts and email address book. Protect your contacts' privacy as well.

D. Network

Implementing network best practices is crucial for maintaining a secure, efficient, and reliable network infrastructure. Whether you're managing a home network or an enterprise-level network, these practices can help ensure optimal performance and security:

- *Network Segmentation*: Divide your network into segments to isolate sensitive data and limit lateral movement for potential attackers.
- *Access Control:* Enforce strict access control policies to limit who can access your network resources. Regularly review and update access permissions. Filter vulnerable websites and network traffic movement especially incoming traffic.
- *Use network security appliances:* Install firewalls at the network perimeter and between network segments. Implement intrusion detection/prevention systems to monitor for and respond to suspicious network activity. Use email filters and web gateways to filter malicious information.
- *Regular Updates and Patch Management:* Keep network devices, routers, switches, and firmware up to date with the latest security patches. Enable automatic updates when available. Keep these appliances up to date with the latest threat intelligence.
- *Network Monitoring:* Continuously monitor network traffic and devices for signs of unusual activity or security breaches. Set up alerts for suspicious events.
- *VLANs (Virtual LANs):* Use VLANs to logically segment your network based on departments, functions, or security levels. VLANs help control broadcast traffic and limit access to specific network segments.
- *Quality of Service (QoS):* Implement QoS policies to prioritize critical network traffic, such as voice and video, over less important traffic. Ensure a consistent and reliable user experience.
- *Backup and Redundancy:* Regularly back up network configurations and critical data. Implement redundancy for key network components to minimize downtime in case of hardware failures.
- *Network Documentation:* Maintain detailed documentation of your network topology, configurations, and policies. This documentation aids troubleshooting and network management.
- *Change Management:* Implement a formal change management process to track and approve network configuration changes. This helps prevent unauthorized or unplanned network modifications.
- *Logging and Log Management:* Enable logging on network devices and centralize log storage and analysis. Logs are invaluable for troubleshooting and detecting security incidents.
- *Wireless Network Security:* Secure your wireless network with strong encryption (WPA3) and a strong passphrase. Implement a guest network for visitors that are separate from the internal network.

- *Regular Security Audits and Vulnerability Scanning:* Conduct periodic security audits and vulnerability assessments to identify weaknesses and remediate them.
- *Network Access Control (NAC):* Implement NAC solutions to enforce security policies for devices connecting to your network, including BYOD (Bring Your Own Device) devices.
- *Compliance and Regulations:* Ensure compliance with relevant industry-specific regulations and standards.

E. Social Media

Social media is a powerful tool for individuals and businesses, but it also comes with certain risks and responsibilities. By following these social media best practices, individuals and businesses can harness the power of social media while minimizing risks and maintaining a positive online presence. Social media is a dynamic space, so it's important to adapt your strategy and practices as platforms and user behaviors evolve. To make the most of your social media presence while staying safe and maintaining a positive online reputation, consider these social media best practices:

- *Privacy Settings*: Review and adjust your privacy settings on each social media platform to control who can see your content.
- *Think Before You Share:* Be cautious about what you share publicly, as even seemingly harmless information can be used maliciously. Consider the potential consequences of your posts before sharing them. Avoid sharing personal information like your home address, phone number, or financial details.
- *Be Mindful of Your Online Persona:* Remember that your online presence can affect your real-life relationships and job prospects. Avoid offensive or controversial content that could harm your reputation.
- *Engage Thoughtfully:* Be respectful and polite in your interactions with others on social media. Constructive criticisms are fine, but avoid engaging in online arguments or trolling.
- *Beware of Phishing and Scams:* Be cautious about clicking on links or opening attachments from unknown sources. Don't share personal or financial information in response to unsolicited messages.
- *Regularly Review Your Friends and Followers:* Periodically review your friends or followers and remove or block anyone who seems suspicious or makes you uncomfortable.
- *Report Abuse and Harassment:* If you encounter harassment or abusive behavior, report it to the social media platform and consider blocking the offender.
- *Stay Informed About Privacy Policies:* Familiarize yourself with the privacy policies and terms of service of the platforms you use.
- *Follow Consistent Branding*: Maintain a consistent brand image as per the institutional tradition and repute across all social media platforms, including profile pictures, cover photos, and bios.
- *Content Strategy:* Develop a content strategy that aligns with the institutional mission and engages your target audience. Create a content calendar to plan and schedule posts in advance.
- *Interact and Engage:* Engage with your audience by responding to comments and messages promptly. Encourage discussions and user-generated content.
- *Use Analytics:* Utilize social media analytics to track the performance of your posts and campaigns. Adjust your strategy based on the data to improve engagement and reach.
- *Crisis Management:* The institute should develop a plan for handling negative comments, social media crises, or public relations issues. Respond to criticism professionally and consider taking contentious discussions offline.

V. CONCLUSION

In conclusion, cybersecurity is essential to protect data, privacy, financial assets, and national interests in an increasingly digital world. It is a proactive and ongoing effort to identify and mitigate vulnerabilities, respond to incidents, and ensure the safety and security of individuals, organizations, and nations. Conducting a survey on cyber hygiene can provide valuable insights into people's knowledge, attitudes, and practices related to cybersecurity. As per the results of the survey conducted at St. Xavier’s College Kolkata, it is understood that there is a need for the HEIs to play a proactive role in awareness towards cyber hygiene amongst all stakeholders and the society at large.

A fundamental principle of cyber hygiene is that it must become a part of everyday routine. Cyber hygiene is about training oneself to form good habits around cybersecurity so that we can stay ahead of cyber threats and online security issues. As with any habit we want to imbed, cyber hygiene requires routine and recurrence. Building a routine around cyber hygiene will help prevent cybercriminals from causing security breaches or stealing personal

information. At the same time cyber security being a highly dynamic concept, we must continuously upgrade the cyber hygiene policies and practices to keep up to the increasing threats in the digital world.

REFERENCES

[1] https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits, last accessed on 02.01.2022, 15:08 hours.

[2] https://www.europol.europa.eu/media-press/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime, last accessed on 02.01.2022, 18:27 hours.

[3] A. Cain, M. E. Edwards, J. D. Still, "An explorative study of cyber hygiene behaviors and knowledge", Journal of Information Security and Applications, 42 (2018), pp. 36-45.

[4] M. Ovelgönne, T. Dumitras, B. A. Prakash, V. S. Subrahmanian, B. Wang, "Understanding the relationship between human behavior and susceptibility to cyber attacks: a data-driven approach", ACM Trans Intel Syst Technol 2017;8(4):51. doi:10.1145/2890509.

[5] L. Shetia, "Managing Cyber Hygiene at a Higher Education Institution in the United States", SAIS 2022 Proceedings.

[6] D. Caputo, S. L. Pfleeger, J. D. Freeman, M. E. Johnson, "Going spear phishing: Exploring embedded training and awareness", IEEE Sec Priv 2014;12(1):28–38. doi:10.1109/MSP.2013.106.

[7] B. Markelj, I. Bernik, "Safe use of mobile devices arises from knowing the threats", J Inf Sec Appl 2015;20:84–9. doi:10.1016/j.jisa.2014.11.001.

[8] Ugwu, A. Casimir, M. Ezema, C. Asogwa, U. Ome, A. Obayi, D. Ebem, C. Olebara, E. Ukwandu, "Towards Determining the Effect of Age and Educational Level on Cyber-Hygiene", 10.1109/NIGERCON54645.2022.9803154.

[9] https://sopa.tulane.edu/blog/cyber-hygiene, last accessed on 03.01.2022, 12:17 hours.