International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

The Importance of Cybersecurity for a Safer Society

***Chapman Eze Nnadozie*[1]*, Mrs. Benisemeni Esther Zakka*[2]**

[1] *Principal Lecturer, Computer Science Department, Abubakar Tatari Ali Polytechnic, Bauchi, Bauchi State, Nigeria*
[2] *Principal Lecturer, Computer Science Department, Federal Polytechnic Bauchi, Bauchi state, Nigeria.*

DOI: https://doi.org/10.55248/gengpi.5.0524.1371

ABSTRACT

The importance of cybersecurity cannot be over-emphasized as our lives revolves round the use of the Internet for several vital services which today is prone to cyberattacks that are predominantly perpetuated by cybercriminals. This paper intends to explore the meaning and importance of cyber security, as well as the possible ways through which one can protect one's device(s) from cyberattacks. The methodology adopted is the use of questionnaire administered on a total of eighty-seven (87) respondents drawn from a higher institution of learning. The findings of this study show that the predominant effect of cyberattacks on the society has instilled some elements of apprehension on the online users thereby making them to be consciously reviewing and updating their security settings to enhance their safety while surfing the net

Keywords: *Cyberattacks, Cybercriminals, Cybersecurity, Importance, Internet, Services.*

1. Introduction

The rapid growth of the Internet technology in recent times has been seen to have a profound influence on our daily lives more than it had ever been in the past. This unfolding rapid momentum in the advancement of the Internet makes it imperative for the society to adopt good cybersecurity strategies in order to protect people's devices from cyberattacks. Cybersecurity is all about safeguarding our data as well as our devices from cyberattacks that can emanate from unscrupulous persons. These attacks are steadily becoming rampant as they often come in form of phishing schemes, data breaches, or even identity theft. [1] [2].

It is notable to all and sundry that access to instantaneous data is key for a more productive society; which today is easily realizable due to the proliferation of internet-ready mobile devices. In this study, the author will be discussing the meaning of cyber security and its related terminologies, the importance of cyber security as well as the possible ways through which one can protect one's device(s) from cyberattacks.

2. Problem Definition

In recent times, cybersecurity has been attracting lots of attention because almost every service we need is in one way or the other requiring the Internet to accomplish it. The rising conviction that the Internet is unsafe makes it imperative for one to understand the importance of cybersecurity for a safer society to douse this apprehension. Therefore, this study intends to delve into the importance of cybersecurity in guaranteeing a safer society.

3. Objectives of the Study

This study intends to –

1. Find out the meaning of cybersecurity/cyberattack.
2. Find out the importance of cyber security for a safer society.
3. Outlay how best our devices can be protected from cyberattacks.

4. Research Questions

The research questions advanced for this study are as follows -

1. What is cybersecurity/cyberattack?
2. What is the importance of cybersecurity for a safer society?

3. What are the ways though which we can protect our devices from cyberattacks?

5. Literature Survey

In exploring the importance of cyber security for a safer society, it is imperative for one to deliberate on the several perspectives of some authors on the key term – cybersecurity. Cybersecurity has been defined in several ways by different authors. [1] defines cybersecurity as the needed “protection to defend internet connected devices and services from malicious attacks by hackers, spammers and cyber criminals”. Cisco, on the other hand, defines cyber security as “the practice of protecting systems, networks and programs from digital attacks” [1], [3]. Elaborating further, [4] highlights that cybersecurity has to do with the internet which entails “the strategies needed to safeguard individual cyber environment” comprising of the persons’ devices, their networks and applications.”

In similar vein, [5] looks at network security and application security as essentials to cybersecurity. It defines network security as “the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware”. On the other hand, application security is seen to focus on “keeping software and devices free from threats”. [6] defines cybersecurity as a means of “protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction”. [7] defines cybersecurity as “preventive methods used to protect information from being stolen, compromised and attacked”. Looking at the various definitions, the underling factor is that cybersecurity is meant to protect one’s devices from cyberattacks.

Cybersecurity evolved over the decades from the use of antivirus kits to fight/protect our devices from virus attacks of the 1990s to the use of Intrusion Detection and Prevention software to guide against worms’ attacks in the early 2000s. From late 2000s till date, cybersecurity has graduated to the inclusion of Application Aware Firewalls as well as Network Flow Analysis software to help identify, squash and prevent cyberattacks [8]. Figure 1 shows the evolution of cybersecurity.

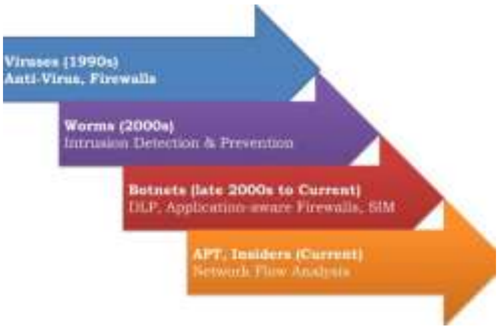
Viruses (1990s)
Anti-Virus, Firewalls
Worms (2000s)
Intrusion Detection & Prevention
Botnets (late 2000s to Current)
DLP, Application-aware Firewalls, SIM
APT, Insiders (Current)
Network Flow Analysis

Fig. 1: Evolution of cyber security [8].

Cyberattack can be defined as “any malicious attempt to gain unauthorized access to a computing system or computer network with the intent to cause damage” Anyone that engages in cyberattack is called a hacker. A hacker is meant to deceitfully penetrate one’s device/computing system to steal the victim’s data for personal gain [9]. The worst of these cyberattacks can be seen as a Denial of Service (DOS) attack. This is a type of cyberattack that portrays a real danger to users in that it can paralyse an internet site from being accessed by its intended users [7]. A cyberattack constitutes a cybercrime.

Cybercrime is perceived as “any unwanted activity involving a computer, device or network” [1]. Similarly, [10] defines cybercrime as an illegal action “committed using a computer and the Internet to steal data and information”. Hacktivism is seen to be a form of hacking often used by online activists for their rights or freedom of expression [11]. A higher dimension to cybercrime is cyberwarfare.

Cyberwarfare can be defined as “an act of waging war on the cyberspace or through the cyberspace”. Cyber espionage, a type of cyberwarfare, refers to the secretive gathering of vital information from a party, under false pretence, for onward delivery to the opposing party. Access is often gained through the stealing of the identity of a legitimate user [11]. All these activities happen in the cyberspace.

Cyberspace is seen as “the environment in which communication over computers network occurs” [12]. A more detailed definition is given by [8] when it defines cyberspace as “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processes and controllers”. [13] portrays several trends to cybersecurity. These trends include the faking of company’s webserver to deceive/defraud people; and the penetration of the cloud space in search of vulnerable devices by hackers.

There are three (3) basic key principles of cyber security. They are confidentiality, integrity and availability. Confidentiality is meant to guarantee that only intended persons can really access sensitive data. Integrity, on its part is meant to ensure that changes to data can only be done by authorized persons. Finally, availability addresses the fact that time is of ultimate importance in the accessing of required data. As such, data should be accessible as at when required without delay. [1] [2] [6].

Cybersecurity can be viewed in three (3) domains – technical, operational and management security. The technical aspect entails the protection of the software and hardware systems from malicious invasions. The operational aspect deals with the safety of the organization’s daily operations. Management security deals with the “governance, strategic planning, policy development and compliance” [7].

There are several types of cybersecurity, notable of which are network security, critical infrastructure, cloud security and application security. Network security is meant to ensure that the organization's or personal network is well configured to avoid any form of bridge in its security architecture. Critical infrastructure of any organization can be targeted and overwhelmed whenever the software used to protect its infrastructure is outdated. The cloud security entails the protection of applications, infrastructure, and data in the cloud. Application security ensures that there are no loopholes in the codes used for designing the website software. However, if any is discovered, it has to be taken care of to avoid security bridges [4].

6. Importance of Cybersecurity

Cybersecurity is crucial for the effective running of any organization. Individuals need cybersecurity to protect their devices and personal information from cyberattacks. For any organization to gain the trust of its customers, the website of such an organization has to be secure to avoid any form of bridges that would lead to loss of viable customer information to cyber criminals [1].

The effectiveness of any cyber secured system entails that the following security measures must be upheld – network security, application security, information security, operational security, end-user security, disaster recovery and business continuity. [14] and [15] highlights that it is dangerous for any organization or individual not to take cybersecurity seriously. As such, it is not the exclusive responsibility of the IT department, rather it is a collective responsibility because a single bridge caused by any member of staff would lead to a cyberattack which eventually affects the entire organization.

Hacking can occur in a very large scale when it is done on a bank infrastructure. [6] highlights an incident that happened in March 2011 against the Commonwealth Bank of Australia which lead to the malfunctioning of their ATM outlets resulting in their incurring tens of thousands of dollars in financial losses. The worsening economic crisis in the globe contributes immensely to the rising trend of cybercrimes, with greed for unjustifiable gains playing a key role [6]. The basic consequences accruable from improper strategic cybersecurity implementation includes financial losses, reputation damage, and legal issues [12].

In summary, the importance of cybersecurity can be seen to include the following key points –

- Upholding the business reputation;
- Saving the business integrity;
- Protecting customers' data from hackers;
- Enabling genuine workers to work from anywhere on behalf the organization;
- Making the organization more efficient and productive;
- Sharing data conveniently without fear of hackers; and
- Making the organization's network always robust due to the fact that it is protected from cyberattacks [16],

7. Cybersecurity Techniques Geared Towards Guaranteeing Effective Protection

There are several techniques that would be undertaken by a user or an organization to ensure that the computing systems are secure from cyberattacks. Five (5) basic techniques as highlighted by [17] are authentication, encryption, digital signature, antivirus, and firewalls. Authentication is seen to be viable through the use of two-factor authentication. This means that you need to use a one-time password in addition to the normal use of password or passcode to log into your account or app. Encryption technique makes your message to be converted to an unreadable form during transmission. On arrival to the recipient, an appropriate unique key is used to decode the message. The key is usually sent through other means from the sender to the recipient. Digital signature involves sending an encrypted message and using another means to send the public key together with the original message. Upon receipt, the recipient decrypts the message using the public key, and compare same with the original copy. If the same, then the message is correct. Antivirus is a software that is used to protect your system from virus attacks. With the auto-protect handle in place, a good level of security is guaranteed. A firewall is a software that can be used to safeguard the systems from cyberattacks. Care must be taken while implementing a firewall to avoid unnecessary delays in the system configuration. A firewall is often installed in the server or client machines.

Furthermore, [7] highlights that the security techniques that can be used to safeguard the systems include firewall, virtual private network (VPN), and intrusion detection. VPN is a very effective way of protecting your systems from cyberattacks. When one is accessing especially a public network, VPN makes the person's online session invisible to other users. That is to say, when an individual is surfing the net using VPN, all the communications becomes confidential. In respect of Intrusion Detection System (IDS), it helps in safeguarding the organization's network by ensuring that all system activities are monitored and any abnormality observed is immediately captured and reported electronically for prompt action to be taken to quash it.

In summary, the actions needed to be taken to protect our data/information are outlined as follows –

- Proper configuration: While using firewall, ensure that the software is properly configured [2]. Improper configuration of the system can lead to the penetration of the system by hackers [18].

- Updated software: Ensure that the installed security apps like anti-spyware, firewall, and antiviruses are frequently meant to be up to date [1], [2], [5], [19].
- Use strong passwords: Always use strong passwords so that it would be difficult to be formulated through guess work. Do not share the password/pin with anybody [1], [2].
- Two-factor password: It is not enough to just use passwords. Add to the security of your device by adopting a two-factor password for your apps [1], [21].
- Scanning: Regularly scan your devices to ensure they are safe [1].
- Save responsively: You need to be mindful of how and where you store vital information [1].
- Be cautious: Always be careful whenever you are communicating online to ensure there are no data breaches. Be sure that the Uniform Resource Locator (URL) of the website is starting with https. [2].
- Access by authorization: System access should be exclusively based on usage by only authorized persons [2].
- Strict compliance to rules: Always be certain that cybersecurity policies are complied with at all times of usage [2].
- Use VPN: It is encouraging to use personal or organizational VPN while surfing the net to ensure privacy of online sessions [1], [2], [19].
- Public networks: Avoid as much as you can the use of public networks. However, if you must do that, ensure that you are browsing in your private VPN [1], [5].
- Avoid links: Be careful to examine every email/link sent to you to ensure they are genuine and safe to open. [1], [5], [20].
- Uninstall: Any software that you go longer need, the best thing to do is to uninstall such software [19].
- Backup data: Always backup your sensitive data [21]. You can do these using applications like iCloud for iPad, and google drive for android devices.
- Bluetooth: It is better to always have your Bluetooth not connected. You should only put it on when you wish to use it [1].
- Verify requests: Be sure to verify requests, especially monetary requests, by insisting on facial contact before proceeding to honour such request.[21].

8. Methodology

The main instrument used in carrying out this research is the use of questionnaire consisting of a total of eleven (11) questions drawn from the three (3) research questions earlier stated. They were administered on eighty-seven (87) respondents comprising of forty-seven (47) students under their parents' sponsorship and forty (40) that are self-sponsored. The author will derive its assertions through the analysis of the responses obtained, and compare same to already existing findings by other authors on the subject matter – Cybersecurity. Table 1 shows the responses of the students in respect of the questions asked.

Sn	Question	Yes	No	Uncertain
1.	Do you understand what the term "cybersecurity" stands for?	54 62%	21 24%	12 14%
2.	Have you ever experienced a cyberattack?	74 85%	9 10%	4 5%
3.	Do you normally feel very safe while surfing the net?	24 28%	59 68%	4 5%
4.	Do you regularly review your device security settings?	71 82%	14 16%	2 2%
5.	Do you regularly update your security software?	62 71%	23 26%	2 2%
6.	Do you see the cybersecurity kits on your device as very effective?	56 64%	25 29%	6 7%

7.	Do you usually use passwords on your files?	59 68%	21 24%	7 8%
8.	Is your computing device(s) password-protected?	63 72%	18 21%	6 7%
9.	Are you using a two-factor authentication on your vital apps?	51 59%	35 40%	1 1%
10.	Do you regularly scan your device(s)?	52 60%	29 33%	6 7%
11.	Do you often backup your essential data?	41 47%	42 48%	4 5%

Table I: Questions and their respective responses.

9. Results and Discussion

This research paper is geared towards ascertaining the importance of cybersecurity towards the building of a safer society. The first three (3) questions are drawn from research questions 1 which seeks to ascertain their understanding on what cybersecurity is. Responses to question 1, which seeks to know whether the respondents understand what the term “cybersecurity” stands for, shows that 54 respondents which represents 62% of all of them know what it means whereas 21 respondents (representing 24%) do not really know but needed more clarification. However, 12 representing 14% of the respondents chose to be indifferent. This first question was meant to get a clearer perspective of the sample on the subject matter. Having gotten the true picture of their understanding, the rest of the questions were answered with more clarity. Question 2 seeks to know whether they have experienced cyberattacks. In response, 85%, 10% and 5% of the respondents answered “yes”, “no”, and “uncertain” respectively. Following this finding, cyberattack can be said to be predominant in the society. Question 3 seeks to know whether they feel safe while browsing. The responses show that only 28% claims that they feel safe while browsing whereas 68% do not feel very safe, and 5% were uncertain. These findings align with the assertions of [1] and [2] when they highlighted that cyberattacks are becoming rampant these days, as they come in form of phishing schemes, data breaches, or even identity theft. Figure 2 shows a bar chart representing the responses obtained in respect of the research question 1.

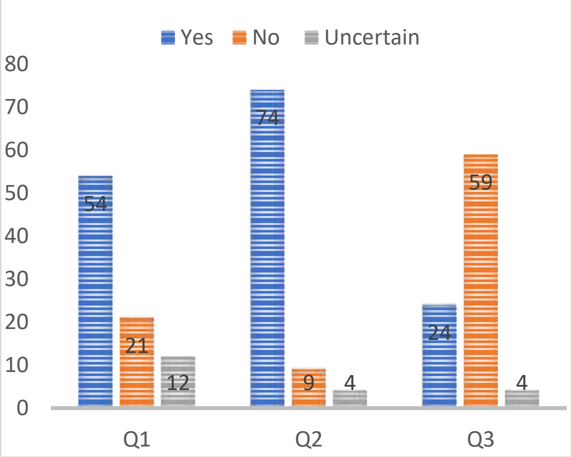

Fig. 2: Responses to questions drawn from research question 1

Questions 4 to 6 seeks to explore the importance of cybersecurity for a safer society. Question 4 seeks to know whether they regularly review their device security settings. The responses show that majority of the respondents do as 71 representing 82% responded in affirmation. However, the 10% that say “no” while 5% were undecided. In respect of question 5 which seeks to know whether their security software is updated regularly, 71% of the respondents do whereas, 26% don’t do that while 2% were undecided. This is encouraging as the finding is in line with the assertions of [1], [2], [5], and [19] which advises individuals to always update their security apps regularly. Question 6 seeks to ascertain the views of the respondents on whether they see the cybersecurity kits on their devices as very effective. The responses show that 64% trust their devices cybersecurity whereas 29% don’t trust their devices cybersecurity. Figure 3 shows a bar chart representing the responses obtained in respect of research question 2.

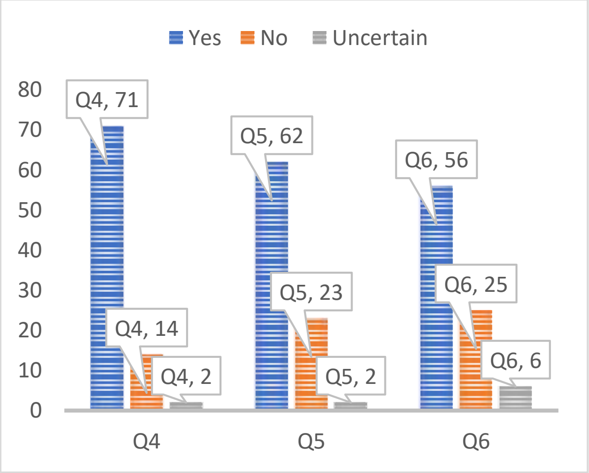

fig. 3: Responses to questions drawn from research question 2

Questions 7 to 11 seek to ascertain the ways through which we can protect our devices from cyberattacks. Question 7 seeks to know whether the respondents normally use passwords on their files. The result shows that 68% do while 24% don't. The remaining 8% were undecided. This finding is in line with the assertions of [1] and [2] which advocate that the use of strong passwords on files in order to make it difficult to be guessed by anyone. Question 8 seeks to know whether their computing devices are password-protected. In response, 72%, 21%, and 7% say "yes", "no" and "uncertain" respectively. This finding is in line with the assertion of [2] which advocates that system access should be strictly based on authentication of its users to ensure that only authorized persons gain access to them. Furthermore, question 9 wishes to ascertain whether they use a two-factor authentication on their vital apps. From the responses, only 59% are doing so while 40% are not taking this security measure. This finding is in line with the assertion of [17] when it says that authentication is viable through the use of a two-factor authentication. This is believed to be an effective security measure that we can add to the mere use of passwords. Question 10 wishes to verify whether they scan their devices regularly, and only 60% of the respondents admit to be doing so. On the contrary, 33% are not regularly scanning their devices for errors or detection of abnormalities while 7% were undecided. The finding shows that there is need for more awareness to be created geared towards educating people on the importance of regularly scanning their devices to enhance the safety of such devices.

Finally, question 11 seeks to know whether they often backup their essential data. Only 47% of the respondents say "yes", while 48% and 5% say "no" and "uncertain" respectively. This finding shows that user education is needed for them to appreciate the need for backups of their essential data to prevent irreparable losses. Fig. 4 shows a bar chart summarizing the responses of the respondents in respect of research question 3.

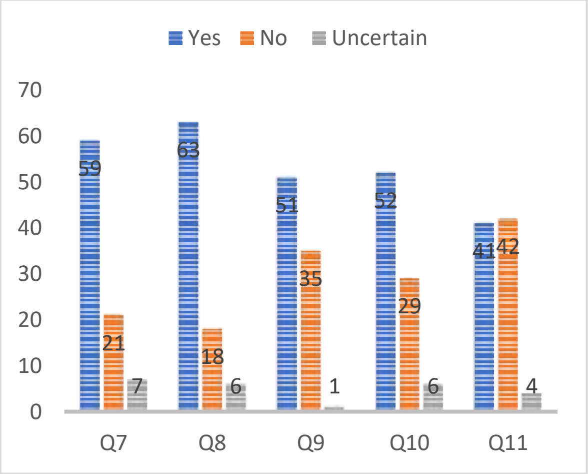

Fig. 4: Responses to questions drawn from research question 3.

10. Conclusion

A sound knowledge of the importance of cybersecurity is vital in enhancing the way we perceive the use of the Internet for vital services. The findings of this study show that -

a) Many have a perceived understanding of the meaning of cybersecurity, but not without more clarity on the concept;

b) Cyberattacks are predominant on the society thereby giving rise to a feeling of an unsafe cyberspace;

c) Majority are poised towards reviewing their cybersecurity settings from time to time to enhance their online safety;

d) Many regularly update their security settings;

e) The use of strong passwords on both files, apps and devices are known, and finally;

f) More awareness needs to be created on the following - the use of two-factor authentication; need for regular device scanning; and need for having essential data backup preferably on the cloud.

11. Recommendation

Based on the findings of this study, the author wishes to recommend the following –

a) Awareness on cybersecurity concepts should be enhanced across the board to promote the safety of our devices and data;

b) Individuals should ensure that they are always using a two-factor authentication for the apps in addition to the use of strong passwords for both their apps and devices;

c) Regular review of your security and privacy settings such as tracking and update of your passwords should be done from time to time to enhance the device security;

d) Regular scanning of your personal devices should be a norm and not seen to be a waste of time;

e) Data backup is essential in guaranteeing your data safety in case of any accidental loss of device or essential data.

References

[1] Kelley, K. (2023). "*What is cybersecurity and why it is important?"*. Available at: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security

[2] Kingsborough.edu (2023). *"Why cyber security is important".* Available at: https://www.kingsborough.edu/its/data_computer_security/documents/why_cyber_security_is_important.pdf

[3] Morgan, L. (2018). "*The importance of cyber security"* Available at: https://www.cpaireland.ie/CPAIreland/media/Education-Training/Study%20Support%20Resources/2019%20Articles/P2-AP-The-Importance-of-Cyber-Security.pdf

[4] Adish, K. et al. (2022). *"A review paper on cyber security",* International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Vol. 2 Issue 2, March 2022, pp. 528 – 531.

[5] Kaspersky Lab. (2023). "*What is cyber security?".* Available at https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

[6} ITU (2022). *"Introduction to security cyberspace, cybercrime, and cybersecurity".* Available at:

https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Introduction%20to%20the%20Concept%20of%20IT%20Security.pdf

[7] Gupta, C. P. & Goyal, K. K. (2020). *"Cybersecurity A self-teaching introduction"* U.S.: Mercury Learning and Information LLC. Available at: https://terrorgum.com/tfox/books/cybersecurityaself-teachingintroduction.pdf

[8] Saraswat, V. K. (2018). "*Cyber Security".* Available at: https://www.niti.gov.in/sites/default/files/201907/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf

[9] Gillis, A. S. & Pratt, M. K. (2023). *"Cyber attack".* Available at: https://www.techtarget.com/searchsecurity/definition/cyber-attack

[10] Zope, A. P. & Chaudhari, R. R. (2022). *"A review paper on cyber security".* In International Journal of Engineering & Technology (IRJET), Volume 09, Issue 8, August 2022, pp. 1561- 1566.

[11] Klopfer, F. et al. (2021). *"Introduction to cybersecurity governance – A tool for members of parliament".*

Available at: https://www.dcaf.ch/sites/default/files/publications/documents/CyberPolicyToolENGLISH.pdf

[12] Bhushan, B. (2023). *"The growing importance of cyber security in the digital age". In* International Journal for Innovative Research in Multidisciplinary Fields, Volume 9, Issue 5, May 2023.

[13] Tabassum, L. & Baker, S. (2020). *"Cybersecurity and safety measures".* Available at: https://www.researchgate.net/publication/342747820_CYBERSECURITY_AND_SAFETY_MEASURES?_tp=eyJjb250ZXh0Ijp7InBhZ2UiOiJwdWJsaWNhdGlvbiIsInByZXZpb3VzUGFnZSI6bnVsbH19

[14] Callejas, J. F., et al. (2021). "*Cybersecurity in the United Nations System Organizations".* Report of the Joint Inspection Unit of the United Nations.

[15] Harney, Julie (2022). *"Users are not stupid: Six security pitfalls overturned". In* Cyber Security: A Peer-Reviewed Journal, Volume 6, Issue 3, pp. 230 – 241, November 2022.

[16] Abdumalikev, G. (2022). "*Profound importance of cyber security on the field of business".* In International Journal on Human Computing Studies, Vol. 04 Issue2, February 2022, pp. 43 – 46.

[17] Pande, J. (2017). *"Introduction to cyber security".* Haldwani: Uttarakhand Open University Available at: https://uou.ac.in/sites/default/files/slm/Introduction-cyber-security.pdf

[18] ThoughLab (2023). *"Cybersecurity solutions for a riskier world".* Available at: https://thoughtlabgroup.com/cyber-solutions-riskier-world/

[19] ASM Technologies Limited (2021). *"Introduction to cyber security (executive summary)".* Available at: https://www.asmltd.com/wp-content/uploads/2017/04/CyberSecurity-1.pdf

[20] Birmingham.gov.UK (2022). "*The importance of cyber security".* Available at: https://www.birmingham.gov.uk/download/downloads/id/15883/the_importance_of_cyber_security.pdf

[21] Brush, K. & Cobb, M. (2024). "*Cybercrime".* Available at: https://www.techtarget.com/searchsecurity/definition/cybercrime