SSRG International Journal of Computer Science and Engineering
ISSN: 2348 – 8387 /doi:10.14445/23488387/IJCSE-V8I11P101

Volume 8 Issue 11, 1-5, Nov 2021

Enhancing Cyber Security Measures For Online Learning Platforms

Vencelin Gino V[1], Amit KR Ghosh[2]

[1,2]*Educational Technology Centre*
The University of Technology and Applied Sciences- IBRA, PO Box 327 Ibra 400
Al Sharqiya North, Sultanate of Oman

Received Date: 03 September 2021
Revised Date: 04 October 2021
Accepted Date: 15 November 2021

Abstract *- Cybersecurity is the mechanism to protect information technology equipment and data from unauthorized access. The most difficult task in today's IT sector is to keep information and data safe from prying eyes. When thinking about cyber security in today's world, the first thing that comes to mind is cybercrime, hacking, and data breaches, which are on the rise day by day. To combat this cybercriminal, all governments around the world are enacting cyber laws [1]. Despite the numerous steps taken to prevent such practices, cybercrime is on the rise. This paper primarily concentrates on the cybersecurity issues that will impact online learning on various platforms. Also, this paper goes over some techniques, policies, and practices that institutions and individuals can use to prevent or protect themselves from cybercriminals.*

Keywords - *Online Learning Platforms, Cyber Security*

I. INTRODUCTION

Industrialization has taken many forms, and it is now in the Information Age of the twenty-first century. Information is wealth, and information defines the world around us. Each individual life is being automated with machines. From our crib – to our bed, all rely on machines. These machines are made up of microprocessors or microcontrollers, which transmit data using radio signals. E-Learning and online learning are considered to be the future learning methods. The high demand for online learning has been shown during the pandemic of Covid-19. In order to promote online learning, adequate protection must be in place to ensure that technology can provide data without manipulation. As a result, it is critical for learners to be aware of security threats and vulnerabilities, as well as the best practices for preventing them because knowledge and understanding of security threat mitigation will assist learners in following best practices and securing their IT-enabled device that can transmit data electronically[2]. It could be a laptop, computer, mobile or tablet pc. In order to begin learning online, first, there is a link to the instructor or facilitator through a network, either wired or wirelessly. As a result, it is important for parents to ensure that the devices given to children are capable of mitigating cybersecurity threats.

II. RESEARCH PROBLEM

Due to Covid-19, online classes have become essential, and it is part of every student's life. Remote learning is enforced to each student during mid of 2020, but not all students have the technology to avail it. Furthermore, there is no defined software or hardware that the students of the institutions use. Every instruction adopted a technology, which is a favor to them in terms of economically and technologically supportive. There is no proper consideration about the end users referred to as students. There was no device defined for students, and no steps were taken to provide end-users with a system that could provide them with the necessary video conferencing features.

Most Video Conferencing Systems are vulnerable and can be hijacked and misused in many ways. Zoombombing and GIF: Account Takeover Vulnerability in Microsoft Teams was commonly reported during 2020 for video conferencing platforms.

The increased number of threats and vulnerabilities is primarily due to the growth of web applications and services. Figure 1 shows vulnerabilities are rising year after year, according to the Common Vulnerabilities and Exposures database.

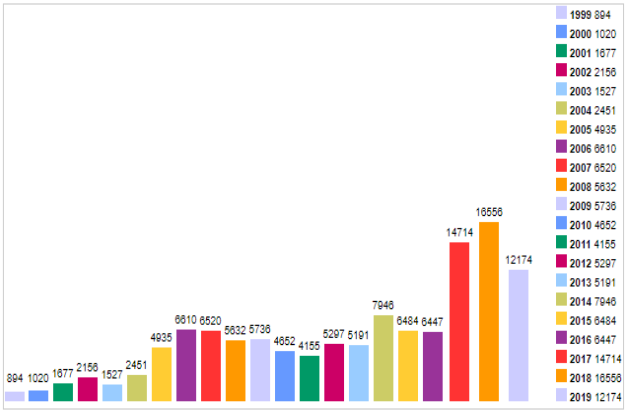

Figure 1:Vulnerabilities by Year [3]

Since remote learning is aimed not just at adults but also at children as young as kindergarten, it is critical to promote cybersecurity initiatives and define a better system that protects the privacy and data of anyone who uses remote learning platforms.[4]

Remote learning is a multilayered technique involving a computerized information system. Malware, Phishing, Denial-of-Service, Session Hijacking and Man-in-the-Middle Attacks, Pharming, and Vishing, are several of the most popular types of cybersecurity attacks that can threaten students who use online learning platforms. This will concentrate on three forms in this article.

1. Account Takeover
2. Data Breaches
3. Cyberbullying

III. RESEARCH OBJECTIVE

- To describe the different types of attacks that can be used against the remote learning platform.
- To raise awareness of the importance of cybersecurity among students, teachers, and parents
- To make remote learning platforms more secure in terms of cybersecurity
- To improve remote learning network cyber security measures.

A. What is Account Takeover?

Account takeover (ATO) is a method of cyberattack in which cybercriminals take unauthorized ownership of other personal accounts using stolen usernames and passwords. By doing that, the cybercriminals gain access to the victims' email, social media sites, e-commerce sites, and other IT-enabled services to make financial and reputation damage to the individual or the business.

B. How does an account takeover happen?

Account takeover relies heavily on social engineering. It's the easiest way to get details out of others. The fraudster contacts the victim via mail, phone, or video conferencing platform and gathers information in order to conduct an account takeover.[5]Social engineering includes

***a) Phishing*:** It is a fraudulent attempt to obtain sensitive information or data, such as usernames, passwords, and credit card details, or other sensitive details, by impersonating oneself as a trustworthy entity in digital communication.

***b) Vishing*:** It is phishing over a telephone system defined as voice and phishing to gain access to private personal and financial information.

***c) Brute-force attack*:** It is a fraudulent attempt in which the attacker submits many passwords or passphrases with the hope of eventually guessing a combination correctly.

d) Bought credentials: Hackers sell credentials in the darknet for cheap, and cyber criminals buy those credentials to gain access to the victims' IT-enabled services.

e) Credential stuffing attacks: It is a type of cyberattack where stolen account credentials typically consisting of lists of usernames and/or email addresses and the corresponding passwords (often from a data breach) are used to gain unauthorized access to user accounts through large-scale automated login requests directed against a web application.

C. How to overcome account takeover?

Account takeover is a vulnerability that the end-user has made, and no program or patch can repair it alone. As a result, training should be provided to students, teachers, and parents about account takeover in order to prevent it. After the end-users have been made aware, education on prevention can be made available to them. Furthermore, a quiz on awareness can give to them to calculate the percentage of each users' understanding of account takeover.[6]Protection against Account takeover is not just the responsibility of the institution or the individual. It is a joint responsibility.

***a) Institutional responsibilities*:** The institution should take responsibility for setting policies for passwords. The password policies can have the following criteria:

- Password should have a minimum length requirement
- Password should have complexity like upper case, lower case, numeric and special characters
- Password must be changed in a given interval
- Multifactor authentication should be enabled
- After a particular number of unsuccessful logins attempt, the user account should be locked and should be unlocked after verification and forced to reset the password
- Lock computing devices if they are idle for more than a given interval
- Enable password history to prevent from using the old password

If you suspect a credential breach or other cyber threat to your network or on any of the devices in your domain, compel all users to change their passwords at the next login to ensure proper security. Additionally, keep the user updated if their IT-enabled device is under threat, based on reports from antivirus portals and other network security gateway devices.[7]

b) Individual responsibilities: Individuals have a critical role to play in avoiding account takeover attacks. To protect their password, they can use the best practices mentioned below.

- Do not divulge your password
- If you feel someone knows your password, then change it with immediate effort
- Do not circumvent password entry with auto logon, application remembering, embedded scripts, or hard code password in applications
- Always lock your IT-enabled devices while not in use
- Do not use dictionary words or acronyms.
- Do not use the same password for multiple accounts

D. What are data Breaches?

Data Breaches are the intentional or unintentional damage, change, or release of secured, confidential, or private information to an untrusted environment. Cybercriminals take advantage of a flaw in an IT-enabled device through software or application and destroy, steal or modify the data. Figure 2 shows the impact of the human factor in IT security and how employees are making businesses vulnerable from within the organization.

Figure 2:Security Risk Survey data [8]

E. How do Data Breaches happen?

Data Breaches due to physical damage to a device or due to natural disaster is not considered cyber threats. Data breaches occur as a result of system vulnerabilities or human error. Human error is said to be responsible for more than 40% of security breaches, according to reports. More than 40% of data breaches can be avoided with proper identity and access control.[9] The most common types of data breaches are hacking, SQL injection, Ransomware, sabotage, malware attack, and denial of service.

F. How to prevent a data breach?

Data breach prevention is a two-way task. Institutions must enforce all access controls, and users must be responsible for and mindful of their actions. Antivirus and antimalware software must also be installed on all IT-enabled devices. The most important things to do to keep data safe are security audits and awareness.

***a) Institutional responsibilities*:** Institutions need to set proper access controls for data and guidelines for the users to prevent data breaches. Data should be available for the concerned person; the confidentiality of the data needs to be maintained; the Integrity of the data should be taken care of with proper settings that can modify it.[10]

- Raising awareness about data breaches among students, teachers, and parents improves protection.
- Informing students, teachers, and parents about data breaches and their implications for protection.
- Track and mitigate malware with antivirus and antimalware software
- Deploy early detection and response tools to detect malicious activities in the systems
- Frequently push updates to IT-enabled devices and track them for potential attacks
- Deploy a system to identify the intrusion
- Request all end-users to report incidents and analyze the incidents and establish a response team to resolve incidents
- Do regular security audits and fix if there is any vulnerability
- Open-source and free software may have glitches or misconfigurations, so test the applications before deploying them and keep them up to date with the new updates.

b) Individual responsibilities: Each person is responsible for the data breach that occurs in the institution as an end-user.[11] As a result, it is critical for each person to adhere to certain guidelines in order to avoid data breaches.

- Sign-out from your applications when they are not in use or when you finished using them
- Protect your IT-enabled devices with a password
- Protect your important files with a password
- Attend all security awareness programs
- Update your software and hardware firmware regularly
- Seek advice from your IT team before you install any new software on your device

G. What is cyberbullying?

Cyberbullying is described as bullying that occurs by the use of an IT-enabled device, such as a smartphone or computer. In social media sites, cyberbullying is more common. Cyberbullying may take place via SMS, comments in social media, personal chat messages, emails, or exchanging content. Cyberbullying occurs when someone uses offensive language, shares, posts, or sends derogatory or negative information about another person. Cyberbullying's primary goal is to humiliate the victim.

H. How does cyberbullying happen?

Cyberbullying occurs when a person feels insecure about themselves. When someone is insecure, he or she uses abusive language or spreads derogatory comments to make others or a rival feel threatened or embarrassed and then feel better. Cyberbullying is more popular on social media platforms, owing to the lack of a moderator or monitoring to inform or regulate users. [9]Figure 3 shows the social media platforms where cyberbullying occurs the most.

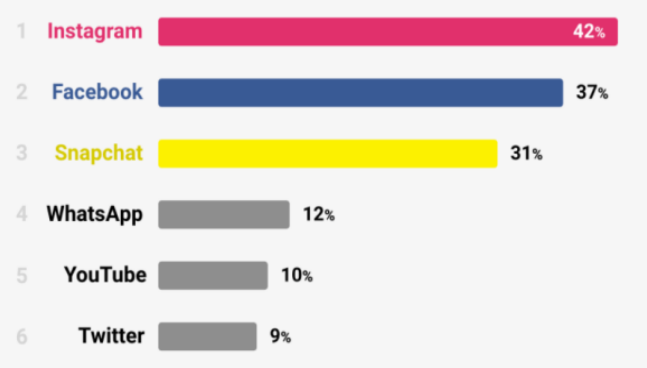

Figure 3: Cyberbullying in social media[12]

I. How to prevent cyberbullying?

Parents should teach their children to accept disappointment and failure rather than blaming or looking for excuses in others. Furthermore, all parents should allow their children to have open conversations with them about what happens in their social media accounts, the reactions of their peers, and how their online or e-learning classes are going so that parents are aware that their child is not a victim of cyberbullying or the cause of it. Moreover, Individuals must take responsibility for their actions on digital media in order to avoid cyberbullying.

a) Institutional responsibilities: Institutions must educate students about the importance of equality and gender neutrality in order for them to recognize that all are the same.

- Organize workshops and conferences to encourage gender equality.
- Make awareness to react favorably to criticism in order to prevent being victimized
- Foster a sense of unity among students by emphasizing that they are all equal in some way
- Remove discrimination and bias in classroom and campus
- Use artificial intelligence (AI) software to track chat, posts, comments, and interactions, and take necessary steps to disable or mask the contents before they are sent to the intended recipient
- Make awareness programs to students about the laws and their effectiveness related to cyberbullying

***b) Individual responsibilities*:** If you don't want to be hit, don't hurt. It is important for parents to teach their children about equality and respect for others in order for them to grow up in a safe community.[13]

- Parents must speak with their children to ensure that they are not victims of cyberbullying or the cause of cyberbullying
- Each student must take responsibility for themselves and should not feel superior or inferior to others
- Rather than criticizing others, students should accept their disappointment and failures and look for ways to improve

III. RESULTS

While most parents and students are aware of cybersecurity threats and their consequences, there are still a significant number of people who are unaware of them. Many devices do not have any safeguards in place to protect them from cyber-attacks. While many of them claim that they do not assume their accounts are being used by others, a small number of people claim that their accounts have been used without their knowledge. Many people have stated that their personal information is not posted in digital media without their knowledge. The vast majority of people said they had never been the victim of cyberbullying.

IV. CONCLUSION

Technology is evolving in education to support the learning and teaching process in a more and more interactive and interesting manner. Due to Covid-19, online learning platforms have become more popular. More IT-enabled devices and applications will be available in the future to aid the teaching and learning process. It is also important that the use of technology in the classroom is to improve and leverage the prototype-based learning process. IT-enabled devices and modern software can provide a more practical method of prototyping and simulation for the learner to understand the concept and visualize them. As a result, there is a significant need to raise awareness and implement proper cybersecurity systems for IT-enabled learning devices.

REFERENCES

[1] Rossouwvon Solms, Johanvan Niekerk., From information security to cyber security, Computers & Security, 38 (2013) 97-102.
[2] Wajeb Gharibi, Maha Shaabi, Cyber threats in social networking websites, Cryptography and Security, (2012).
[3] Vulnerabilities by Date https://www.cvedetails.com/browse-by-date.php
[4] Vipin Kumar, Jaideep Srivastava, Aleksandar Lazarevic, Managing Cyber Threats: Issues, Approaches, and Challenges, Springer
[5] Seung Hyun Kim, Qiu-Hong Wang, Johannes B. Ullrich, A comparative study of cyberattacks, Communications of the ACM, 55(3) (2012).
[6] Robin Gray, Account Takeover (ATO) attacks and how to prevent them, (2021).
[7] Tara Kissoon, Optimum spending on cybersecurity measures, Transforming Government: People, Process and Policy, (2020).
[8] The Human Factor in IT Security https://www.kaspersky.com/blog/the-human-factor-in-it-security

[9] Carmen Reinicke, The biggest cybersecurity risk to US businesses is employee negligence study says, (2018),
[10] Hansde Bruijn, MarijnJanssen, Building Cybersecurity Awareness: The need for evidence-based framing strategies, Government Information Quarterly, 34(1) (2017) 1-7.
[11] Ravi Sen, Sharad Borle, Estimating the Contextual Risk of Data Breach: An Empirical Approach, Journal of Management Information Systems,32 (2015).
[12] Ogi Djuraskovic, Cyberbullying Statistics, Facts, and Trends
[13] Robert Slonjea, Peter K.Smitha, Ann Frisénb, The nature of cyberbullying, and strategies for prevention, Computers in Human Behavior, 29(1) (2013) 26-32.