Security Risks and Challenges of Remote Working and Learning

Sheyla Gyles
Computer Science Department
Hampton University
Hampton, VA
(Faculty Advisor: Dr. Chutima Boonthum-Denecke)

Abstract – This report will discuss and analyze the risks and different challenges which are accompanied when completing remote work and learning. Specifically, this paper will focus on this trends' effect, during the 2019 Coronavirus pandemic (COVID-19). The different applications that will be included in this research are Slack, Zoom, Skype, Microsoft Teams, Google Meets, Trello, Webex, and Troop Messenger. In recent months, there has been a complete increase in the amount of people worldwide that use these platforms. However, the majority of users do not fully understand security and privacy when using these different platforms. Due to this lack of knowledge, this comes with an increase in attacks. This study will further discuss the different pros and cons of each of the different platforms (mentioned above); the applications that have been breached, how often they were breached, different flaws, vulnerabilities of each system and more. This study coherently uses and assesses its credibility with the assistance of research, a user survey, and past research studies on this topic.

I. Introduction

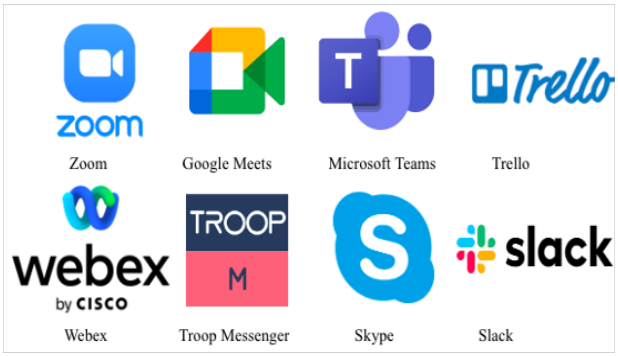


Figure 1: Remote Working Platforms [3]

The coronavirus pandemic, also referred to commonly as COVID-19, is an airborne disease caused by the SARS-CoV-2 strand [2] and is a unique makeup of the influenza virus. Due to the rapid outbreak of this airborne infection, many businesses, agencies, and organizations were posed with numerous challenges. The most significant challenge during this pandemic was that people could not be face to face in any physical setting. There were many rules and regulations put into place to ensure physical distancing and safety measures. As a result, however, many companies had to implement "remote working" strategies in order to mitigate the contamination of the virus while simultaneously creating an effective action plan to continue the flow of work needed to be done within the realm of the organization. The solution to this was the creation and use of video communication and group messaging applications. These applications were used more than ever before and has carried its importance to today post the pandemic. These applications were created as a means to send data over an

organization's network privately as well as conduct video conferencing methods within the workplace. As its use has increased, there have been various efforts attempted to ensure “full” security to ensure that these applications are safe, there are many areas that have loopholes and it is imperative for not only users to be aware in order to protect their personal data, and data from their trusted organization. Safety and security are left not only to the user, but to the developers and employees who create these applications. The most common “remote working” applications that arose from the pandemic include Slack, Zoom, Skype, Microsoft Teams, Google Meets, Trello, Webex, and Troop Messenger. Companies that use these different applications have reasons in which they prefer the one that they use over the others. Reasons can range from the compatibility/integration with other applications, its overall runtime, its dedication to security and privacy, compatibility on various operating systems (Windows, macOS, Linux, etc.), or if a VPN is provided/integrated with the application.

A. Problem Statement

With the recent and full emergence of video communication and group messaging tools/applications during the 2019 Coronavirus pandemic. These communication applications have been used more than ever. However, as more companies use these public platforms, there is room for data loss and modifications in the hands of intruders. CEO’s and the risk management team of these communication applications are now forced to create more elaborate security methods in order to prevent data from being stolen from its users as there has been an increase in security and face privacy breaches. These application vendors are now doing everything in their power to ensure security/privacy of its users. These vendors, however, should not be the only people taking action to stop this from happening. Human error is one of the most dangerous cyber breaches that an organization face [7]. It is important for users to understand privacy and security as well as how to keep these applications safe.

II. Methodology

This study will use a combination of literature review and user surveys to collect data and gather results related to the conducted thesis. The methodology is explained as follows:

A. Literature Review

This goal of this paper aims to explore and discuss the security and privacy issues that arise when using these remote working video communication applications, both generally speaking and in relation to the eight applications of most popular usage between communication applications. I will also go into detail about the advantages and disadvantages of the system applications for the population and business/agency usage.

Through this literature review, details about how organizations use these applications and what they get out of the specifications of each application is imperative. With this understanding, I can then use scholarly literature and research papers to provide a foundation for building on research in order to support my findings drawn from data collected from the created remote working communication user surveys.

Video communication tools are application software in which is used by two parties in order to communicate via audio and video using internet connection [17]. These tools enable the two communicating parties to be able to initiate live conferences and distant meetings via audio input, video input and the usage of text transmission. It is imperative that the applications consider the security and privacy of

the specific application that the company chooses to work with.

Security and Privacy:

Privacy is the understanding of how a user decides to provide their personal information store, use, and access this sensitive data. [9]. Security on the other hand is the issue that needs to be resolved by developers; This refers to the way that personal information is safeguarded when utilizing these remote working/ video communication services. [11]. These communication applications have integrated security systems in order to ensure that their users are safe from hackers, third parties and any other malicious incomings.

Extensions, also referred to as add ons or plugins are used in order to enhance the experience of the application. A few of the different add-ons that are used commonly today include Slack extension, Calendy, Assana, G Suite, Teleparty, and Krisp.ai just to name a few. In addition to enhancing the users experience of the application and providing productivity features to the clients, on a business perspective it is beneficial as well as it allows the applications company to know that the application is of continuous use. For example, the Slack plug in on Zoom allows users to be able to view their work messaging channel in real time, which can later be used for company understanding and personal reasons. Another example of this is the YouTube extension, an addon which allows users to watch videos from the YouTube application clearly it synchronizes the video playback for everyone in order to prevent glitching and lagging issues. Like the remote application, the security and privacy of the add ons is not solely the responsibility of the providers of the service but it is ultimately up to the user to grasp understanding of security practices.

Security Implementation:

Security vulnerabilities is another grand topic of concern when speaking about the privacy and security implementation of remote video conferencing applications. Hackers leverage the current capability in the communication application to achieve the numerous of malicious things.

To make these platforms secure, there have been different methods of implementation including virtual desktops, authentication actions, VPN, etc. in order to challenge the intruder in their attempts to override the system or disrupt users. In order for these hackers to get into the system, they use the abuse of public functionality as an essential entry point in order to exploit cross application request forgery, flaws, and denial of service attacks. To further discuss security and privacy in an academic and professional setting, it is important to assess the threats that hackers exploit. Everything mentioned above regarding these vulnerabilities and implementation are considered to be principal in the process to remove these security issues.

As a user, there are different areas that are imperative to understand while using these platforms in order to protect the personal data of both the user and the organization. This is where the problem ties in. However, these applications' security and privacy is not only left to the user/employed organization but also the company that provides the applications creation itself. The most common platforms used are Citrix, Microsoft Teams, and Zoom. Companies who partner with these organizations have different reasons for their use with the company, but it comes down to the security/privacy and the UI/UX interface of the application.

Within the different platforms there are various plugins also referred to as extensions that allow users to enhance their experience with the application both personally and professionally. Each application has their own plug-ins and

browsers/Operating Systems (OS) that react better with each. For example, within the Zoom platform there is an application which allows the user to be able to merge their applications with their integrated Microsoft Office tools.

With the modern rise of technology, remote working tools that enable individuals and teams to collaborate securely and effectively are becoming increasingly popular. By providing features like file transfers, video conferencing, screen sharing and others, these tools make it easy for workers to access the necessary tools to stay connected and enable them to access content and collaborate no matter where they are located.

Advantages in Video Communication:

One of the primary advantages of remote working video communication is its convenience; by using a platform that allows you to put yourself in a space of virtualness, beyond the pandemic, this has allowed employees to be able to take their work home.

Remote working tools can offer many benefits to businesses, employees, and clients alike- especially in the current virtual climate. Remote tools are technology-based, often cloud-based, systems that allow organizations to facilitate remote working arrangements simply and securely [26]. Remote working tools provide businesses with flexibility to set up and adjust remote working conditions for their employees in an efficient and secure way. Some tools, such as video conferencing systems, email, and project management software, allow employees to collaborate and communicate effectively, whereas other tools exist to streamline tasks like task organization and time tracking [20]. In addition, there are also benefits for clients- as remote tools help keep businesses running and support both employee and client satisfaction [10]. Ultimately, remote working tools are vital in the modern work environment, as they offer a safe and secure way to facilitate remote working arrangements and have numerous benefits to businesses and clients [16]

Disadvantage in Video Communication:

While there are many different advantages in the realm of video communication usage on a technological perspective as well as user efficiency. There are also many disadvantages on those two schemes of entity.

From a technical standpoint, there are specific security and privacy risks associated with video calls. As the communication apps are used through the internet, there are many different DNS (Domain Name Server) [8] hijacking where hackers can breach into your security and cause a great deal of harm. The hackers can redirect you traffic to receive information from it. In addition to the idea of hacking, when these calls are hacked, sensitive information can be intercepted or recorded without the user's knowledge or consent. Malware is another technical flaw, video conferencing software can be targeted by malware, which can infect a user's device and compromise personal and sensitive information. There is also Phishing where scammers can use video conferencing as a tool to phish for personal and financial information, such as login credentials and credit card numbers. Finally, there is Lack of encryption: Some video conferencing tools may not have proper encryption in place, which can leave sensitive information vulnerable to interception. To mitigate these risks, it's important to use secure video conferencing software, keep software up to date, use a secure internet connection, and be vigilant about phishing scams and suspicious activity. It is important to note that users play an enormous role in the protection of data, and it is not solely up to the software engineers/ security teams of the applications companies.

B. User Surveys

Data will be collected from users of various remote working platforms through the conduction of a survey. The purpose of this survey will be to understand and educate users of the most used platforms, how well users understand their privacy and security on these applications, and their experience with hacking that has occurred while using these applications. There will be an analysis of the findings from the survey along with the other sources of information to make conclusions and recommend possible solutions to the different issues mentioned above within the thesis.

III. Results

This section will cover and a compass the different results from the methodology that has been outline within section II. After reading and analyzing all my results I have notices that a lot of my survey results came out as predicted, and I had a total of 108 participants.

As far as the first question being *"Out of the 8 most used remote communication applications, which ones do you currently use?"*. For this survey question, the "applicant" was able to choose more than one answer. Zoom was the most commonly used video communication application with 96.3% (103 respondents) saying that they primarily use Zoom. The Skype Communication application was followed up

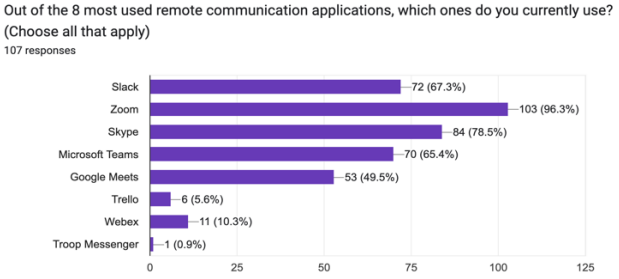


Figure 2: Remote Communication Usage

Having 78.5% of the votes (84 respondents), thirdly the Slack Communication application had 67.3% of the votes (72 respondents) and the other applications that followed were Microsoft teams 65.4% (70 respondents), Google Meets 49.5% (53 respondents), Webex 10.3% (11 respondents), Trello 5.6% (6 respondents) and finally, the most unpopular application, Troop Messenger 0.9% (1 respondent).

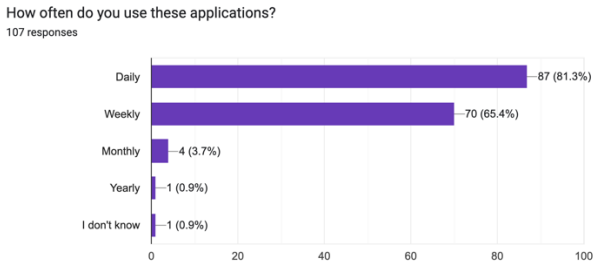
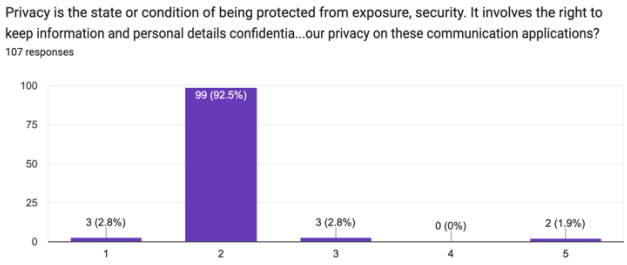


Figure 3: Application Frequency

For the second question *"How often do you use these applications?"*, Respondents were given four different time choices. Daily, Weekly, Monthly, and I don't know.

Daily was given 81.3% (87 respondents), weekly was given 65.4% (70 respondents), monthly had 3.7% (4 respondents), yearly had 0.9% (1 respondent) and I don't know had 0.9% (1 respondent).

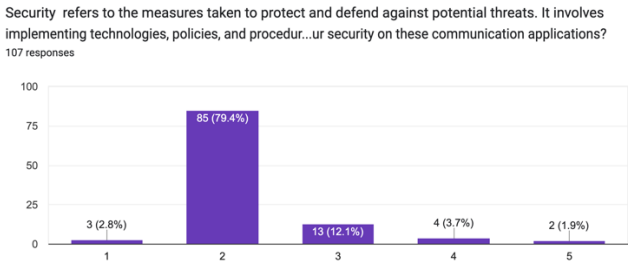
Figure 4: Privacy



For the third question *"Privacy is the state or condition of being protected from exposure, security. It involves the right to keep information and personal details confidential. On a scale of (1-5) how often do you think about your privacy on these communication applications?"*. For this question 1 was not at all on the range to 5 all the time.

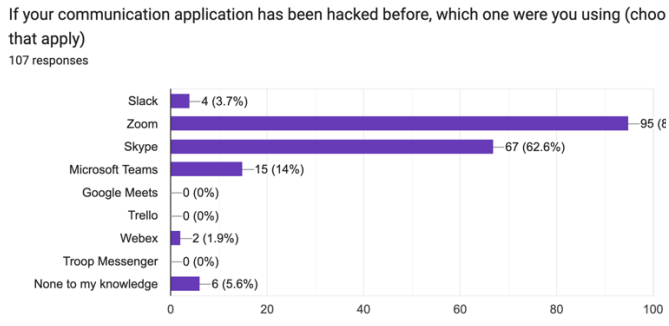
For this question the majority supported 2 as their answer. This was 99 respondents (92.5%), and the other options had the same votes.

Figure 5: Security



For the fourth question, *"Security refers to the measures taken to protect and defend against potential threats. It involves implementing technologies, policies, and procedures to safeguard against potential risks and ensure the confidentiality, integrity, and availability of assets. On a scale of (1-5) how often do you think about your security on these communication applications?"*. In this scale 1 was not at all on the range to 5 all the time. Just like the privacy question, it was the same amount of support. 2 as their answer which attracted 79.4%, which is 85 respondents, and the other options were very unpopular.

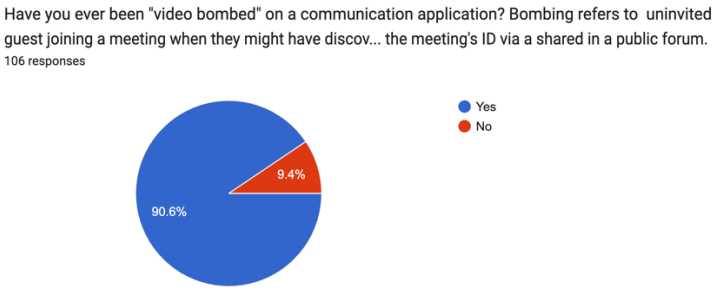
Figure 6: Remote Applications Hacked



For the fifth question, *"Have you ever been "video bombed" on a communication application? Bombing refers to uninvited guest joining a meeting when they might have discovered the meeting's ID via a shared in a public forum."*.

For this question, many options were available to be selected, just like question 1. For this, Zoom once again was the top choice, 88.8% (95 respondents), Skype once again following up62.6% (67 respondents), running up with Microsoft Teams 14% (15 respondents), None to their knowledge 5.6% (6 respondents), 0 for Google Meets and Trello, Slack with 3.7% (4 respondents), and finally Webex 1.9% (2 respondents).

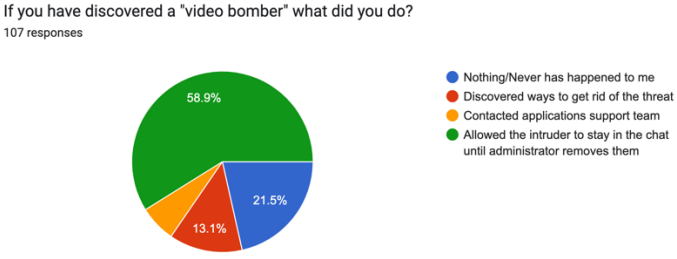
Figure 7: Video Bombing



For the sixth question, *"Have you ever been "video bombed" on a communication application? Bombing refers to uninvited guest joining a meeting when they might have discovered the meeting's ID via a shared in a public forum."*.

This question had two options and 106 responses answered. 90.6% of the respondents said yes, and 9.4% said no.

Figure 8: Video Bombing Response

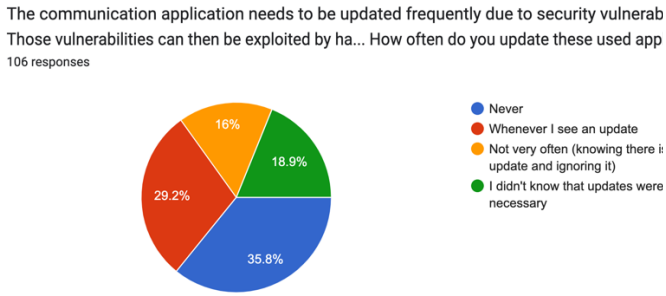


For the seventh question, *"If you have discovered a "video bomber" what did you do?"*.

The respondents were given the choices Nothing/Never has happened to me, discovered ways to get rid of the threat, contacted applications support team, Allowed the intruder to stay in the chat until administrator removes them.

58.9% chose the option “Allowed the intruder to stay in the chat until administer removes them”, 21.5% chose the option “Nothing/Never has happened to me”, 13.1% chose the option “discovered ways to get rid of threat”, and the rest of the percentage, chose “Contacted the applications support team”.

Figure 9: Application Updates

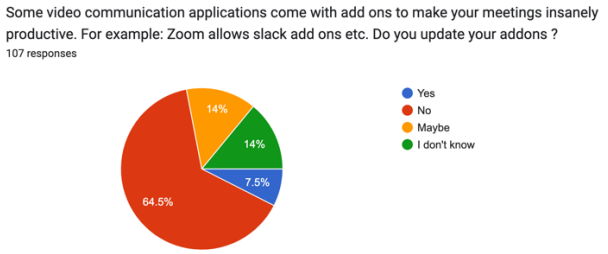


For the eighth question, *“The communication application needs to be updated frequently due to security vulnerabilities. Those vulnerabilities can then be exploited by hackers. How often do you update these used applications?”*.

Respondents were given four different options. “Never, Whenever I see an update, not very often (knowing there is an update and ignoring it), and I didn’t know that updates were necessary.”

The first option had 35.8% “never”, the second option “Whenever I see an update” had 29.2%, the third option “I didn’t know that updates were necessary” 18.9%, and finally “Not very often (knowing there is an update and ignoring it) 16%”.

Figure 8: Extension Updates

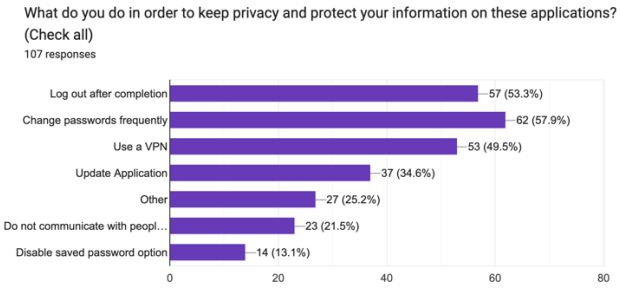


For the ninth question, *“Some video communication applications come with add ons to make your meetings insanely productive. For example: Zoom allows slack to add ons etc. Do you update your addons?”*.

The respondents were given a few different options.

Yes, no, Maybe, I don’t know. The most popular choice was No with 64.5%, Maybe with 14%, I don’t know with 14% and Yes with 7.5%

Figure 10: Add on updates



Finally, the last question that was asked was *“What do you do in order to keep privacy and protect your information on these applications? (Check all)”*. This question like mentioned gave a lot of different choices to choose from including
Log out after completion, change passwords frequently, use a VPN, Update Application, Other, do not communicate with people that you do not know, and disable saved password option

As far as the results, the most popular means of protection was changing password frequently. This had 57.9% and 62 respondents, following was log out after completion with 53.3% and 57

respondents, and thirdly was use a VPN which had 49.5% with 53 respondents. The others that followed were update application 34.6% (37 respondents), other 27 respondents (25.2%), do not communication with people you do not know with 21.5% (23 respondents), and finally Disable saved password option which was (13.1%) which is 14 different respondents.

IV. Analysis

Like mentioned before, most of the results came out as expected. For the first question I had made sure that people were aware of specific remote applications. Due to the Coronavirus pandemic, there were about 90% of participants who were using 2 or more of the different eight applications provided. For the second question, I took it a step further to ask which application out of the ones given were susceptible to hacking. Out of the choices, the majority application that was selected was Skype and Zoom. For the third and fourth question I asked the about security and privacy to be able to allow people to not only understand the concept as well as see how aware people are of it applied. There was a grand percentage of people who, however, didn't get this question right. This was surprising, especially considering that the 21st century sits primarily on the use of technology. The fourth and fifth questions were tasked to ask what one would do in a situation where they were tasked with dealing with an intruder, majority of people said that they would leave the intruder until the administrator is notified. These questions created an understanding of people's lack of knowledge in relation to technology. My recommendation is that Hampton University should require students to take a course related to a computer science before stepping on campus. This process would be change the way in which students interact with electronics on a day to day and be aware of the dangers.

V. Conclusion

Remote working has become increasingly popular since the implementation of various work-from-home norms. To facilitate the process, virtual collaboration tools such as Zoom, Google Hangouts and Microsoft Teams have become staples for remote working [15]. Zoom offers the most comprehensive set of features for both enterprise users and small businesses. It provides audio, visual, and live streaming capabilities that other tools lack. Google Hangouts is a more budget-friendly option as it provides more limited features than more expensive tools such as Zoom. It is suitable for casual conversations and meetings. Microsoft Teams provides a more integrated and organized digital work environment. Its user-friendly interface allows users to collaborate on tasks and documents in real time [13]. Therefore, it is important to select the right tool to suit the specific needs of the organization. The internet can be a great resource for accessing information, chat rooms, finding entertainment, and more. But it is important to remember that it is also not secure, and vital personal and financial information should never be stored online. For example, studies have shown that as many as 80% of websites are vulnerable to data breaches [12]. Therefore, it is essential to take necessary precautions when transmitting or storing data online, such as utilizing encrypted networks and passwords, to minimize the risk of being exploited [14].

ACKNOWLEDGEMENTS

This work is partly supported by the National Science Foundation CyberCorps: Scholarship for Service program.

References

[1] Association of Computing Machinery, "ACM Code of Ethics and Professional Conduct," 22 January 2019. [Online]. Available:

https://ethics.acm.org/code-of-ethics/. [Accessed 09 December 2022].

[2] CDC, "Centers for Disease Control and Prevention," 26 January 2023. [Online]. Available: https://www.cdc.gov/coronavirus/2019-ncov/index.html. [Accessed 29 January 2023].

[3] Owen, Artist, *Remote Working Platforms.* [Art]. Coderus, 2021.

[4] Indeed Editorial Team, "Indeed," 02 April 2022. [Online]. Available: https://www.indeed.com/career-advice/career-development/video-conferencing-tools. [Accessed 12 December 2022].

[5] J. Nurse, N. Williams, E. Collins, N. Panteli, J. Blythe and B. Koppelman, "Remote Working Pre- and Post-COVID-19: An Analysis of New Threats and Risks to Security and Privacy," *Internation Conference on Human Computer Interaction*, vol. 1421, pp. 583-590, 2021.

[6] P. Satam, K. Hairiri and S. Hariri, "Anomaly behavior analysis of website vulnerability and security," i*nternational Conference of Computer Systems and Applications*, vol. 13, pp. 300-314, 2016.

[7] Forbes Editorial Team, "15 Must-Have Features Of A Successful, User-Friendly Mobile App," 12 August 2022. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2021/05/24/15-must-have-features-of-a-successful-user-friendly-mobile-app/?sh=22d74c8a6a7a. [Accessed 01 January 2023].

[8] NIST, "NIST," 19 June 2022. [Online]. Available: https://csrc.nist.gov/glossary/term/computer_security. [Accessed 2022 20 November].

[9] S. J. Bigelow, "Data Privacy (Information Privacy)," 10 August 2022. [Online]. Available: https://www.techtarget.com/searchcio/definition/data-privacy-information-privacy. [Accessed 18 November 2022].

[10] VMware, "What is remote work security?" 19 September 2022. [Online]. Available: https://www.vmware.com/topics/glossary/content/remote-work-security.html. [Accessed 08 December 2022].

[11] Citrix, "What is Remote Work Security?" 02 February 2022. [Online]. Available: https://www.citrix.com/solutions/secure-access/what-is-remote-work-security.html. [Accessed 12 January 2022].

[12] G. Henseke and A. Felstead, "Assessing the growth of remote working and its consequences for effort, well-being and work-life balance," *New Technology, Work and Employement*, vol. 32, no. 3, pp. 195-212, 2021.

[13] B. Wiederhold, "Connecting Through Technology During the Coronavirus Disease 2019 Pandemic: Avoiding “Zoom Fatigue”," *Cyberpsychology Behavior and Social Networking*, vol. 23, no. 7, pp. 437-438, 2020.

[14] IEEE, "Business Process as a Service: Chances for Remote Auditing," *Annual Computer Software Application*, vol. 35th, no. 5, pp. 18-22, 2019.

[15] D. Blechynden, "Best remote desktop software of 2023," 02 November 2022. [Online]. Available: https://www.techradar.com/news/best-remote-desktop-software. [Accessed 12 October 2022].

[16] A. William, "The Pros and Cons of Working Remotely," 15 March 2022. [Online]. Available: https://trainingmag.com/the-pros-and-cons-of-working-remotely/. [Accessed 04 November 2022].

[17] R. Madell, "Pros and Cons of Working From Home," 30 June 2022. [Online]. Available: https://money.usnews.com/money/blogs/outside-voices-careers/articles/pros-and-cons-of-working-from-home. [Accessed 15 September 2022].

[18] A. Stevens, "Advantages and Disadvantages of Remote Work," 16 July 2021. [Online]. Available: https://www.techtarget.com/whatis/feature/15-advantages-and-disadvantages-of-remote-work. [Accessed 19 November 2022].

[19] Team Building, "Remote Work Software," 17 July 2022. [Online]. Available: https://teambuilding.com/blog/remote-work-software. [Accessed 04 December 2022].

[20] Kaspersky, "Cyber Security Risks: Best Practices for Working from Home and Remotely," 20 July 2022. [Online]. Available: https://usa.kaspersky.com/resource-center/threats/remote-working-how-to-stay-safe. [Accessed 19 November 2022].

[21] P. Nicolleti, "Remote work security statistics in 2022," 31 March 2022. [Online]. Available: https://www.cybertalk.org/2022/03/31/remote-work-security-statistics-in-2022/#:~:text=One%20report%20showed%20that%2020,the%20breach%20or%20malware%20attack.. [Accessed 10 January 2022].

[22] CyberRisk&Stats, "Statistics Of Cyber Security Risks When Working from Home," 09 January 2021. [Online]. Available: https://www.dbxuk.com/statistics/cyber-security-risks-wfh. [Accessed 2022 October 2022].

[23] J. P. Mello, "Remote Work Heightens Privacy and Security Anxiety Among Employees," 12 January 2022. [Online]. Available: https://www.technewsworld.com/story/remote-work-heightens-privacy-and-security-anxiety-among-employees-87411.html. [Accessed 2023 09 January].

[24] Andy Sto, "What Are the Most Common Remote Work Security Risks?," 20 July 2021. [Online]. Available: https://andysto.com/what-are-the-most-common-remote-work-security-risks/. [Accessed 21 November 2022].

[25] I. Arghire, "Cisco Webex Vulnerability Allows Ghost Access to Meetings," 19 November 2020. [Online]. Available: https://www.securityweek.com/cisco-webex-vulnerability-allows-ghost-access-meetings/#:~:text=Identified%20by%20IBM's%20security%20researchers,email%20addresses%20and%20IP%20addresses).. [Accessed 07 July 2022].

[26] A. Alam, "How to Make Sure Your Remote Team Isn't a Cybersecurity Threat?," 03 March 2022. [Online]. Available: troopmessenger.com/blogs/cybersecurity-threat. [Accessed 12 December 2022].

[27] C. Peoples, "Undermining Microsoft Teams Security by Mining Tokens," 13 September 2022. [Online]. Available: https://www.vectra.ai/blogpost/undermining-microsoft-teams-security-by-mining-tokens#:~:text=In%20August%202022%2C%20the%20Vectra,their%20plaintext%20storage%20on%20disk.. [Accessed 10 December 2022].

[28] OXY Occidental College, "Settings to Prevent Zoom-Bombing," 13 July 2022. [Online]. Available: https://www.oxy.edu/offices-services/its/services/video-conferencing/settings-prevent-zoom-bombing. [Accessed 02 December 2022].

[29] O. Freire, "How to Overcome the Security Challenges of Using Slack for Your Enterprise," 17 November 2022. [Online]. Available: https://www.safeguardcyber.com/blog/security/how-to-overcome-the-security-and-compliance-challenges-of-using-slack-for-team-collaboration#:~:text=One%20of%20Slack's%20security%20issues,and%20channels%20on%20the%20platform.. [Accessed 12 December 2022].

[30] C. Osborne, "Skype ‘spoofing vulnerabilities’ are a haven for social engineering attacks, security researcher claims," 05 February 2021. [Online]. Available: https://portswigger.net/daily-swig/skype-spoofing-vulnerabilities-are-a-haven-for-social-engineering-attacks-security-researcher-claims. [Accessed 13 January 2023].

[31] Devoteam, "Security & privacy in Google Meet Video Conferencing," 21 November 2022. [Online]. Available: https://gcloud.devoteam.com/blog/securit-privacy-in-google-meet-video-conferencing/#:~:text=You%20need%20to%20be%20aware,that%20you%20store%20in%20Drive.. [Accessed 13 December 2022].