Faculty of Computational Sciences & Informatics - Academic City University College, Accra, Ghana
Society for Multidisciplinary & Advanced Research Techniques (SMART)
Trinity University, Lagos, Nigeria
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
Harmarth Global Educational Services
ICT University Foundations USA
IEEE Computer Society Nigeria Chapter

Proceedings of the 36th iSTEAMS Accra Bespoke Multidisciplinary Innovations Conference

Cybersecurity and Mental Health in the Digital Age

[1]Talabi, A.A., [2]Longe, O.B., [3]Muhammad, A.A. & [4]Olusanya, K.
[1]African Centre of Excellence in Technology Enhanced Learning, NOUN - Abuja, Nigeria
Faculty of Computational Sciences, Academic City University College, Accra, Ghana
Department of Computer Science, Kaduna State University, Kaduna, Nigeria
Industry Expert from ISACA Ibadan, Oyo State, Nigeria
E-mails: doyin.talabi@gmail.com; olumide.longe@acity.edu.gh; muhdaminu@kasu.edu.ng; kunlesanya2002@gmail.com

ABSTRACT

More than half of the world population is connected through the Internet and end users and professionals alike spend many hours on it to communicate, research, work, collaborate and socialize, generating millions of bytes of data daily. Cybercriminals are also taking the advantage to hack systems and steal or corrupt data, disrupt operations and the level and intensity cyber-attacks have increased tremendously, since the Russia invasion of Ukraine. Individuals who have been affected by cybersecurity breaches have been known to develop increased anxiety levels, fear of others online, leading to depression. Cybersecurity professionals are also under pressure to perform and continually prevent attacks and protect information assets. Many of these incident responders have experienced workplace stress, burnout, depression, suicidal thoughts and quitting the cybersecurity industry due to pressures to keep away all cyber- attacks. All these scenarios of cybersecurity breaches have implications on mental health. This paper did a systematic review to find correlations between cybersecurity and mental health. The findings revealed that as a result of cybersecurity breaches, both users and professionals have developed mental health conditions including anxiety, stress, burnout, depression, suicide thoughts and professionals quitting the industry and further increasing the skills shortage. The paper concluded that there is a positive correlation between cybersecurity breaches and mental health and we should all be conscious of this and balance our work-life lifestyle; employers should encourage discussions around mental health, provide counselling services and invest in cybersecurity resources and further education to motivate professional staff and reduce cybersecurity skills shortage.

Keywords: Anxiety, Burnout, Cybercrime, Cybersecurity, Depression, Digital Age, Mental Health, Stress,

Proceedings Citation Format
Talabi, A.A., Longe, O.B., Muhammad, A.A. & Olusanya, K. (2023): Cybersecurity and Mental Health in the Digital Age. Proceedings of the 36th iSTEAMS Accra Bespoke Multidisciplinary Innovations Conference. University of Ghana/Academic City University College, Accra, Ghana. 31st May – 2nd June, 2023. Pp 35-44. https://www.isteams.net/ghanabespoke2023 dx.doi.org/10.22624/AIMS/ACCRABESPOKE2023P4

1. BACKGROUND TO THE STUDY

There has been exponential growth in the use of the internet expanding the concept of the world as a global village with up to 5.4 billion users (68%) out of 7.9 billion estimated world population having access to the internet, as at June 2022 according to (intenetworldstats,2022). Access to the internet has led to the global development and use of computers, mobile devices and software applications in different areas of endeavours and across platforms, affecting our lives socially, officially, politically, publicly and privately. (Zaryn, 2022)

There are many positive uses of the Internet that have been of immense benefit to the society and affected our daily lives. These include fast and enhanced communication, education and research. However, there are many negative uses of the same platform to the detriment of individuals, business and government. These include hacking, identity theft, cyber-attacks and cyber-bullying affecting self- esteem, addiction leading to insomnia, increase in stress levels, depression which can result in mental health conditions that affect the mental health of users and professionals. All these have increased the importance of protecting and securing information assets including the human users(Devloper,2021).

2. STATEMENT OF THE PROBLEM

The world has become an inter-connected society through the pervasiveness and convergence of channels, platforms, applications and networks through the internet. COVID-19 pandemic increased the pace of digital transformation of many organisations and service providers such many services are provided as contact-less and self-service solutions without human interaction, with use of chatbots and remote working has become normal. There has also been a sharp increase in cybersecurity breaches resulting in identity theft, ransomware attacks, disruption of operations and loss of income. All these tend to increase fear and anxiety levels of users and also put pressure on cybersecurity professionals to perform and secure information assets. This has led to stress, depression, burnout and certain cybersecurity professionals quitting the industry. It has therefore become important to look at the effects and implications cybersecurity breaches on mental health of users and cybersecurity professionals (Pan American Health Organisation, 2022). The importance of this study is further reinforced by the sheer number of people using the internet. For example, as at November 2022, an estimated 6.6 billion users have smartphones according to (oberlo,2022). These has multiplied the number of attack surfaces that to be secured from cybercriminals and cybersecurity breaches.

3. OBJECTIVE

The objective of the research paper is to raise the level of awareness about the relationship between cybersecurity and mental health in this information age that we are in. This is because of its negative effects and implications on the mental health of both non-technical users and professionals. The recommendations would enable us develop best practices and behaviour that would ensure work-balance between the use of Information Technology in the digital age and reduce the negative effects on our mental health.

4. METHODOLOGY

The approach of this paper is to undertake a systematic review of different research works done on cybersecurity and its relationship with mental health. The literature review will include effect on children, end users and cybersecurity professionals for ease of analysis and making appropriate recommendations for each group.

5. THEORETICAL FRAMEWORK (SHATTERED ASSUMPTIONS THEORY)

According to **Janoff-Bulman's** Shattered Assumptions Theory, each individual has three assumptions about the world and self; the world is meaningful, the world is a benevolent place and the self is worthy. However, when an individual experiences a traumatic event like a cyberattack or cybersecurity breach, they question these assumptions in the light of their experiences and this causes the assumptions to **shatter** and can make the individual have a negative perception of the world and themselves. This is believed to be the cause of posttraumatic stress disorder (PTSD) symptoms (Schuler, 2013)

6. DEFINITIONS

According to the World Health Organization (WHO), mental health is a "state of well-being in which the individual realizes his or her own abilities, can cope with the normal stresses of life, can work productively and fruitfully, and is able to make a contribution to his or her community". It has also been proved by research that there is a high risk of having other diseases if the mental disorders are not taken care of and may result in unintentional and intentional injury (Pan American Health Assciation,2022).

"A mental disorder is characterized by a clinically significant disturbance in an individual's cognition, emotional regulation, or behaviour. It is usually associated with distress or impairment in important areas of functioning. Mental health condition is a broader term covering mental disorders, psychosocial disabilities and (other) mental states associated with significant distress, impairment in functioning, or risk of self-harm" (World Health Organisation,2021).

"Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber-attacks. It aims to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, networks, and technologies." (IT Governance,2022)

A Cybersecurity breach is any incident that results in authorized access to data, systems, applications and devices. Occurs when a hacker bypasses security controls in place. Examples of breaches include when Marriot Hotels announced a breach affecting up to 500 million customers in 2018 and in 2019, AVAST, an antivirus production company was hacked when a cybercriminal compromised an employee's VPN credentials(Kaspersky,2022)

Cybercrime is the act of using or targeting computers or related devices to carry out a criminal activity. This could be done for financial, political or personal reasons. Examples of cybercrime include identity theft, theft of financial data or card, email fraud and ransomware. (Kaspersky,2022).

7. LITERATURE REVIEW

7.1 Internet Usage Statistics

The table below summarizes the sheer number of internet users and highlights the level of activities and the number of systems, laptops, computers and attack surfaces to be protected by cybersecurity professionals and also explains why cybercriminals are interested in hacking and underscores the importance of cybersecurity controls to avoid cybersecurity breaches which can lead to mental health conditions (Wpbeginner,2022)

Table 1: Internet Usage Statistics

1	General Usage Statistics	i. ii. iii.	There are about 5.4 billion internet users worldwide as at June 2022, which is about 68.3% penetration, but 2.5 billion are still without access. The most popular language used is English, followed by Chinese and Spanish. 32% of internet users are between 25 and 34 years' old
2	Mobile Usage Statistics	i. ii. iii.	90% of global internet population access the internet through a mobile device Mobile internet traffic accounts for 55% of web traffic TikTok app was the most downloaded in 2021 with 656 million downloads
3	Website and Domain Statistics	i. ii.	Over 1.5 billion websites hosted on the internet, but only 200 million are active There are over 370.7 million domain names registered globally with China having the largest number, 8.8 million or 33.80% global share
4	Social media and email usage statistics	i. ii. iii. iv. v.	Over 93% of internet users or 4.65 billion are social media users There over 4.1 billion email accounts registered worldwide. 99% of email users check their email every day, sometimes up to 20 times a day 40% of 18 year olds open their email on their mobile device 58% of users check their emails before reading news on social media

According to the 2022 (ISC)2 Cybersecurity Workforce Study, the cybersecurity workforce is an estimated 4.7 million professionals, but there is still a global shortage of 3.4 million workers in the field (Children's bureau, 2019).

7.2 Effects of Cybercrime and Cybersecurity on Mental Health

According to the children's bureau (lake, 2022), there are significant risks associated with the increased usage of technology by children. The amount of screen time and use of social media have been linked to mental health conditions and internet addiction has become a major issue among teenagers. This has been linked to depression, low self-esteem, loneliness and reduced physical activity. Since it is impossible to avoid use of technology these days, it is imperative to monitor children and limit the time spent on social media or looking at a screen. Common warning signs in teens an adolescents include difficult time concentrating, extreme mood swings, feeling sad or withdrawn, severe changes in sleeping habits, personality traits, behaviour and partaking in risky behaviour that can lead to harming them or others.

Victims of cybercrime are known to experience physical, emotional and financial trauma. They find it difficult to trust anyone online and also feel guilty and complain of insomnia and eating disorders. Where personal data have been breached and resulted in embarrassment or harassment, victims feel vulnerable and may turn to alcohol and drugs for relief. These can result in anxiety and depression(Sripriya,2020) , which are types of mental health conditions.

According to a Forbes report (Winder,2022) , a survey of more than 1,000 cybersecurity professionals across Europe and the United States of America found that 50.8% have been prescribed medications for their mental health. Between July 2021 and June 2022, 27% confirmed that their mental health had declined and 64% confirming that mental health issues have impacted their ability to get work done. Professionals have been experiencing stress, anxiety, burnout, depression even before the COVID pandemic and considered suicide. The job of a cybersecurity professional is highly rewarding but very stressful.

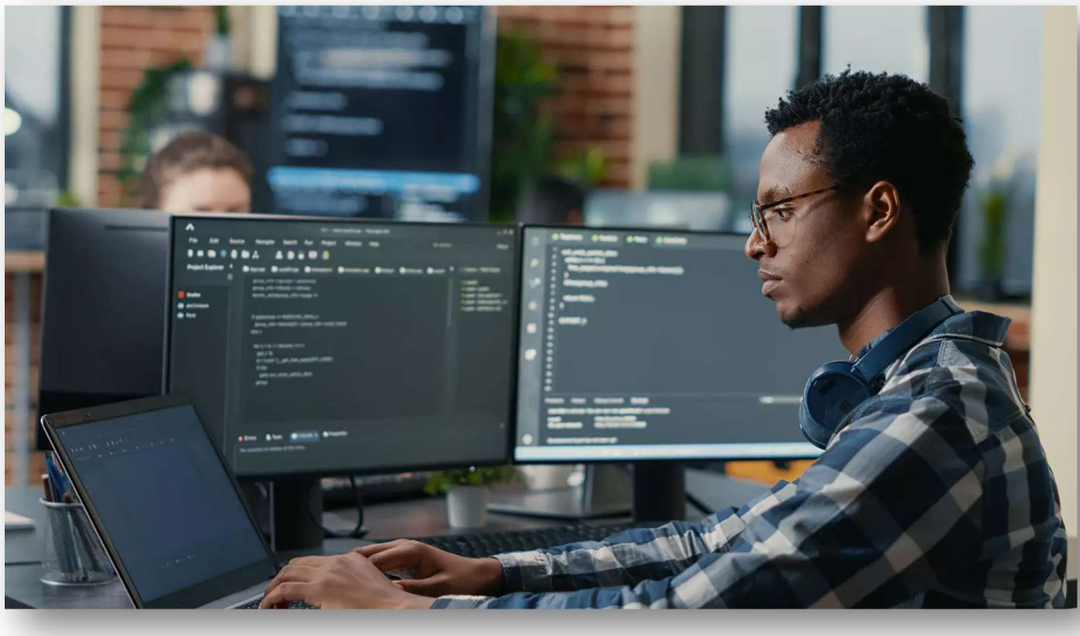

Fig 1: Cyberworks – Computer Usage
Source: https://www.weforum.org/agenda/2022/03/closing-the-cybersecurity-skills-gap/

The job is unpredictable as adversaries continue to improve their tools and techniques at a dynamic rate and there is a constant feeling of not knowing where the next incident would be from and these definitely affects their mental health condition. There is also the rush to implement new digital processes to protect the business to prevent cybercriminals taking advantage of vulnerabilities.

Also, cybersecurity professionals working remotely with low budgets and inadequate infrastructure struggle to keep up and perform, feel isolated with negative effects on their mental health. Work-life balance is recommended as one of the ways to cope with mental health issues. Cybersecurity professionals are also expected to remain vigilant even after work hours which affects personal time and leads to unmanaged workplace stress leading to burnout and want to leave the industry because of that. Many cybersecurity professionals suffering from mental health conditions resort to unhealthy coping mechanisms like alcohol and suicidal thoughts.

The authors recommended that professionals should share their experience with professionals who can give coping tips and techniques, exercise and set daily routines including sleep time, talk openly about mental health issues and choose empowerment over shame. They should also stop doom scrolling on social media and set personal boundaries and realistic goals. Employers should also have employee assistance services for mental health, stress and related issues. According to the NETACEA (2022) report, cybersecurity job is stressful and can affect mental health because the responsibility is to protect the business from cyberattacks which can affect reputation, continuity and profits. According to the research, 91% of cybersecurity professionals reported that their work- related stress levels increased over the past year and 45% have considered quitting their jobs due to stress.

There are three stressful factors that affect cybersecurity work. These are Shortage of cybersecurity staff leading to job overload, the expectation to be constantly on call and the impossibility of stopping every cyber threat. The pressure to perform and stop all attacks is one of the greatest reasons for professional staff anxiety and burnout. There is also a retention problem and many professionals are leaving because of the immense pressure and stress of the job. This results in further skill gaps, because of slow replacement, putting further pressure on workload of staff and the stress increases. Cybersecurity Professionals cope with the stressed work environment but still need support to remain focused, healthy and productive. Working remotely has it is advantages, but there are cases the isolation of staff affects their mental health.

The practice of working with online conference software has its advantages, but has resulted in unguarded speech by certain users, resulting in cyber bullying which can lead to loss of productivity, illness, absenteeism and more stress. This can happen where there are no formal organizational structures in place or there is team conflict. In such cases, it might be better to leave to avoid developing mental health conditions. The authors recommended ways to improve mental health to include investing in cybersecurity and providing budget, resources and skilled staff to protect the business; Board and management staff should improve their knowledge of cybersecurity and take cyber threats seriously.

Organizations should put in place support and counselling resources for professionals who want to improve their mental health and others; Organizations should introduce wellbeing programs for professionals and all staff to improve employee retention and productivity; Businesses can appoint mental health champions and create an environment where mental health issues are discussed; Every employee should be conscious of the interpretation and effect of online posts and confirm they are not hurtful before sending them; Cybersecurity professionals should learn to take a break from social media and not take everything they read online as being true.

According to zdnet.com report(Palmer,2022), cybersecurity work is considered stressful, many professionals are feeling burnout and considering leaving their jobs. The research reported that according to research by VMWare, 47% of cybersecurity responders experienced burnout over the past 12 months, but the percentage is slightly down from 51% in 2021. Cybersecurity professionals need to avert threats from gangs and state sponsored groups and ensure their end users have up-to-date tools to stay safe within controlled budgets and teams. They also have to manage vulnerabilities, zero-day exploits. It was also reported that cyber-attacks have increased since the Russia invasion of Ukraine. Hybrid working conditions, brought to the fore by the COVID pandemic, with its own advantages also brought additional cybersecurity challenges that cybercriminals can exploit. These has increased pressure on cybersecurity professionals to perform, even with fewer number of staff. To reduce effects of burnout, many organisations are implementing strategies to help cybersecurity professionals balance their work-home life with flexible hours of work, access to therapy and coaching and investment in further education.

ETACTICS (Clark,2021) reported that 56% of people say that technology at work reduces in-person interaction, that for every 10% increase in negative social media interaction, the risk of depression increases by 20%, Excessive use of smartphones cause sleep problems and leads to depression, Technology use can result in reduced physical activity and around 3.2 million deaths occur per year as a result. Those who spend over 8 hours per day on a computer are likely to have moderate or high levels of depression. Like everything, use technology in moderation to help manage its negative impacts

There are positive effects of technology on mental health. Technology provides tools to help our mental health. According to (Clark, 2021) Tele medicine has helped to increase access to mental care services and virtual therapy now possible better than before the COVID19 pandemic. This has helped to optimize the use of the few specialists in this area. Many mental health apps have also been created to ease access from a mobile device and online care have proved successful. Health information systems are becoming popular and attracting developers and investors.

8. DISCUSSION OF FINDINGS

Exposure of children to the internet and mobile devices pose a risk of mental health conditions including depression, low self-esteem, feeling of loneliness, lack of physical activity and difficulty in concentrating arising from internet addiction and extended social media use. There are about 5.4 billion internet users worldwide as at June 2022 and 32% of them are between 25 and 34 years' old. 90% of global internet population access the internet through a mobile device and mobile internet traffic accounts for 55% of web traffic. 93% of internet users or 4.65 billion are social media users. There over 4.1 billion email accounts registered worldwide and 99% of email users check their email every day, sometimes up to 20 times a day. 40% of 18 year olds open their email on their mobile device. 200 million of the 1.5 billion websites hosted on the internet are active. The above scenario translates to a lot of online activities, for both genuine and criminal transactions. Cybersecurity professionals have been estimated to be around 4.7 million professionals, with a global shortage of 3.4 million workers in the field, putting tremendous pressure on cybersecurity professionals to perform and secure systems from cybercriminals who want to hack systems and cause cybersecurity breaches and other consequential incidents.

This will definitely put personal and corporate data at risk and cybersecurity breaches have been recorded. The Forbes reports confirmed that 50.8% of cybersecurity professionals have been prescribed medications for their mental health and 27% confirmed that their mental health had declined with 64% conforming that mental health issues have impacted their ability to get work done. Professionals have been experiencing stress, anxiety, burnout, depression. All the reports conformed that the job is stressful due to pressure, job overload due to skills shortage, expectation to be constantly on call and the impossibility of stopping every cyber threat.

There is also a retention problem and many professionals are leaving because of the immense pressure and stress of the job, further increasing the shortage and stress levels. Also, cybersecurity professionals working remotely with low budgets and inadequate infrastructure, suffer from isolation and struggle to keep up and perform with negative effects on their mental health. The mental health conditions common among cybersecurity professionals include anxiety, burnout, eating and sleeping disorders resulting in depression and thoughts of suicide and leaving the cybersecurity industry.

However, technology has certain positive impact on mental health. Tele medicine provides easy access to mental care services in different geographical areas, allowing the optimal use of the few professionals and many mental health apps have been developed to provide access through the mobile phone. Health information systems development have been boosted and is attracting developers and investors.

9. RECOMMENDATIONS

In the case of children and teenagers, it is recommended that time spent on the internet, social media or looking at a screen should be monitored and controlled since we cannot avoid the use of technology these days. Children should also be educated about the benefits as well dangers of social media, taught how to keep their profiles private and not engage strangers online. Awareness training on best data privacy and protection practices, indicators of cybercrime and cyber-attacks should be given to users to avoid loss of personal and financial data that can lead to financial losses and reputational issues that can cause trauma leading to mental health conditions like fear, anxiety, depression and loss of trust in others.

A lot of different measures and approaches can be taken in the case of cybersecurity professionals. These will include provision of counselling services, appointing mental health champions, encouraging discussion around mental health in organizations, allowing flexible work hours, increased education and hiring and training of new cybersecurity professionals to replace quitting staff and beef up the skills shortage. On a personal level, cybersecurity professionals should be encouraged to set personal boundaries, ensure work-life balance, keep in touch with colleagues and family even when working remotely, seek for external support when needed, avoid unhealthy habits of turning to drugs and alcohol and take breaks from the internet and social media.

10. CONCLUSION

The systematic review of the correlation between cybersecurity and mental health has indeed shown to be a positive one. The number of devices, systems connected globally and the millions of data generated daily confirmed the high level of activities on the internet. Cybercriminals are also known to have launched cyber-attacks on individuals, groups and government. The research showed that these cyber-attacks have resulted in cybersecurity breaches of personal, financial and corporate data with loss of money, business and reputation. Cybersecurity professionals are also under pressure to prevent to perform and prevent these attacks. All the above cause trauma for everyone affected leading to fear, anxiety, loss of trust, stress, burnout, suicidal thoughts depression which are mental health conditions.

REFERENCES

1. Children's bureau. (2019). effects of technology on mental health https://www.all4kids.org/news/blog/effects-of-technology-on-mental-health/(Accessed 26/11/2022)
2. Clark, M (2021). 19 Negative Effects of Technology on Mental Health https://etactics.com/blog/negative-effects-of-technology-on-mental-health (Accessed 27/11/2022)
3. Clark, M (2021). 22 Surprisingly Positive Effects of Technology on Mental Health https://etactics.com/blog/positive-effects-of-technology-on-mental-health (Accessed 27/11/2022)
4. Dave Devloper (2021). the positive and negative effects of the internet on our daily lives https://community.thriveglobal.com/the-positive-and-negative-effects-of-the-internet-on-our-daily-lives/ (Accessed 25/11/2022)
5. Dentzel, Zaryn. (2022) "How the Internet Has Changed Everyday Life." In Ch@nge: 19 Key Essays on How the Internet Is Changing Our Lives. Madrid: BBVA, 2013 https://www.bbvaopenmind.com/en/articles/internet-changed-everyday-life/ (Accessed 25/11/2022)
6. IT Governance (2022). What is Cybersecurity https://www.itgovernance.co.uk/what-is-cybersecurity
7. Kaspersky (2022). What is a security breach https://www.kaspersky.com/resource-center/threats/what-is-a-security-breach (Accessed 27/11/2022)
8. Kaspersky (2022). What is cybercrime https://www.kaspersky.com/resource-center/threats/what-is-cybercrime (Accessed 25/11/2022)
9. Lake S (2022). The cybersecurity industry is short 3.4 million workers—that's good news for cyber wages. https://fortune.com/education/business/articles/2022/10/20/the-cybersecurity-industry-is-short-3-4-million-workers-thats-good-news-for-cyber-wages/ (Accessed 27/11/2022)
10. Miniwatts Marketing Group (2022). Worldwide internet usage and Population Statistics 2022 estimates https://www.internetworldstats.com/ (Accessed 25/11/2022)
11. Netacea (2022). Does Working in Cybersecurity Pose Risks to Mental Health? https://netacea.com/blog/working-in-cybersecurity-risks-mental-health/ (accessed 26/11/2022)
12. Oberlo (2022). how many people have smartphones https://www.oberlo.com/statistics/how-many-people-have-smartphones (Accessed 25/11/2022)
13. Palmer, D (2022). Your cybersecurity staff are burned out - and many have thought about quitting/https://www.zdnet.com/education/professional-development/your-cybersecurity-staff-are-burned-out-and-many-of-them-have-thought-about-quitting/ (accessed 26/11/2022)
14. Pan American Health Organisation. Mental health (2022) https://www.paho.org/en/topics/mental-health (accessed 24/11/2022)
15. Pan American Health Organisation. mental health and covid19 (2022).https://www.paho.org/en/mental-health-and-covid-19 (accessed 24/11/2022)

16. Schuler, Eric Robert. (2013). The Glass Is Neither Half Full Nor Empty, It Is Shattered: a Prospective Study of Shattered Assumptions Theory and Psychological Flexibility, thesis, December 2013; Denton, Texas. (https://digital.library.unt.edu/ark:/67531/metadc407756/: accessed November 26, 2022)
17. Sripriya V.(2020). effect of cybercrime on mental health. https://www.linkedin.com/pulse/effect-cyber-crime-mental-health-sripriya-v/(Accessed 26/11/2022)
18. Winder, D (2022) mental health in cybersecurity 51% of workers takes meds, me included https://www.forbes.com/sites/daveywinder/2022/06/08/mental-health-in-cybersecurity-51-of-workers-take-meds-me-included/ (Accessed 26/11/2022)
19. World health organization. (2021). Mental disorders https://www.who.int/news-room/fact-sheets/detail/mental-disorders: mental disorder is characterized ,different types of mental disorders. (Accessed 25/11/2022)
20. Wpbeginner. (2022). Internet usage statistics and latest trends. https://www.wpbeginner.com/research/internet-usage-statistics-and-latest-trends/ (Accessed 26/11/2022)