RESEARCH ARTICLE OPEN ACCESS

Cybersecurity: Risks of Internet Exposure to Kids

God'salvation Fechukwu Oguibe

ABSTRACT

Technological advancement in recent time has laid the foundation for numerous innovations in the way internet is being used in daily endeavors. This ranges from widely acceptable adoption of the social media into mainstream media, to several innovations, paving way for a variety of devices to have the internet protocol (IP), including smart cities and homes. Although the trends in the internet technology are mostly beneficial to humanity, there are risks and hazards associated to these disruptions, used as enablers to perpetuate crimes. Regardless of age and demography, all and sundry are prone to the brunt of internet crimes but a special attention is drawn to the younger population (ages 3-18 years) who are amongst the most vulnerable according to some studies. This technical report presents leading research on the various pitfall of internet crimes as they impact on children when exposed to uncontrolled internet access and also feasible solutions are being discussed to address the most prominent of the issues highlighted in this paper. Some suggested approaches to curbing the internet menace are also preferred.

Keywords: - Cybersecurity, vulnerability, youngsters/children, Internet, Social media, Internet games, Cyberattack, Cyber bullying

I. INTRODUCTION

Advancement in technology has facilitated better approaches to mitigating cyber-attacks yet, the same technology provides opportunity for hackers to create more ingenious tactics of compromising the security systems on the internet. Increasingly, children and adolescents are exposed to the internet as part of everyday live [1]. A similar study suggests that preschoolers become familiar with digital devices before they are exposed to books [2]. This significantly shows reduction in the age of first exposure to internet being a contributory factor to the increasing number of youngsters being exposed to theinternet.

As a reaction to the ever-growing engagement of the young on the internet over the recent years there has been increase and consolidation of effort amongst researchers on the correlation between emotional and mental well-being of children exposed to the internet. Although there are limited publications about the impact of the internet on children, substantial evidence points at alarming demerits which require urgent intervention. The risk associated to early exposure to internet include both criminal and psychological effects.

A number of factors are responsible for the increase in the rate of cyber-attacks. These influences include digital transformation and the commercial model of more people doing business over the internet. This age of technological advancement has led to an increasing need to transact on the internet. Our way of life is increasingly online. This paradigm shift does not exclude the children as their daily need to access the internet is ever increasing. For instance, during the COVID 19 pandemic, there was proliferation of virtual classes paving way for the youngest of school children to have access to the internet daily.

Policy enactment and enforcement are crucial to the ubiquity of internet technology today, this is essential to assess and verity the impact of exposure to the internet amongst children and further guide policies for cautious and effective use amongst these vulnerable population. The mitigation approach to reducing the impact of cyber-crime on children should be founded in research and evidence based to enable adequate monitoring and evaluation of strategies implemented.

Children, just like the adults are notimmune to common cyberattack and cyber threats which include all events which could jeopardize the confidentiality, integrity, or availability of digital information or information systems. Common forms of threats in the cyber space include; Phishing, the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons like executing and propagating malicious content by being disguised as a trustworthy entity in electronic communication [3]. A keylogger is a common form of malicious software that records every keystroke the victim makes on the computer. Keyloggers are a type of spyware, malware designed to spy on victims. Because they can capture everything you type, keyloggers are one of the most invasive forms of malware [4].

This paper is primarily focused on vulnerabilities that exists as a result of innocence and naivety of a child being exposed to the internet.

II. LITERATURE REVIEW

a. *Technology use in young people*

Children have more access to the internet in recent time than in the past. In counties with high rates of connectivity, young people aged 15-24 form a majority of persons online in comparison to other ages of the online population [5]. There is a clear preference for gaming, chatting and social media use amongst the younger population. According to research, 92% of American youths asked said they use the internet daily, with 24% reporting they use it "nearly constantly." [6].

b. *Effects of online video games on children*

There are different perspectives to the impact of internet video game on children; this is a major concern because there are both subtle and insidious effect of this form of internet exposure. Internet games are usually addictive, thus, interacting with games, and their “addictive” tendency is a downside of child internet exposure which usually manifests as “Internet Gaming Disorder” (IGD) and was recently included in the Appendix of the Diagnostic and

Statistical Manual of Mental Disorders. According to [3, 10], Some important brain regions are adversely affected by internet gaming, such brain centers include those responsible for reward, impulse control and sensorimotor co-ordination and thus can reduce child’s productivity, impact negatively on emotion control and increase tendency of obsessive-compulsive behaviors in children.

c. *Children and the social media*

Over the years the intensity of virtual interaction and socialization has increased amongst children, a recent study estimated and suggested that over 90% of young people are using social media every hour of the daily [7]. Texting is a commonest form of daily communication in adolescence, as are mediums such as instant messaging, social media platforms and video chatting [6]. Studies shows that relationships are initiated and developed amongst children mainly through the social media, however, on the other hand, using a computer to study or for recreation time has been negatively associated with time with friends. This places social media on the watchlist of child internet usage as a risk.

d. Cyberbullying

Although cyberbullying is being underestimated by many parents, it is a common form of bullying enhanced by advancement in technology and increase in the use of smart-phones. The increasing use of the social media amongst children provides the avenue for virtual/cyber bullying which is constantly perpetuated irrespective of geographical location. Cyberbullying has a cascaded effect on the parents of the affected. Most bullying are performed via email where threatening messages are being sent causing harassment. This occurs via instant messaging, chat rooms, Instagram, tiktok, text messaging and some web platforms created for the sole purpose of bullying. Other forms of cyberbullying are orchestrated in voting booth where kids and teenagers vote others as being 'ugly', 'too short' or 'too fat'. All these forms of bullying occur as a result of inadequate monitoring of children activities online.

III. INTERNET FRAUD/SCAMS

Fraud amongst adults is very common. However, a dangerous yet underestimated form of fraud is one that rides upon the naivety and vulnerability of the younger population. To take advantage of those who are weak and in an undiscerning age group is undoubtedly one of the most heinous crimes. Children at younger ages may increasingly become the victims of online fraudsters when interacting with electronics for pleasure, education, or socialization. Children frequently need their own accounts created by their parents but accessible by them alone in order to participate on these networks [8]. They become impeded by this pattern, and occasionally becomes victims of fraud. The common forms of fraud amongst the children include identity theft through social engineering, and phishing, Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons like executing and propagating malicious content by being disguised as a trustworthy entity in electronic communication [9]. The resultant effect is obtaining of parent’s credit card information through the child by the fraudsters.

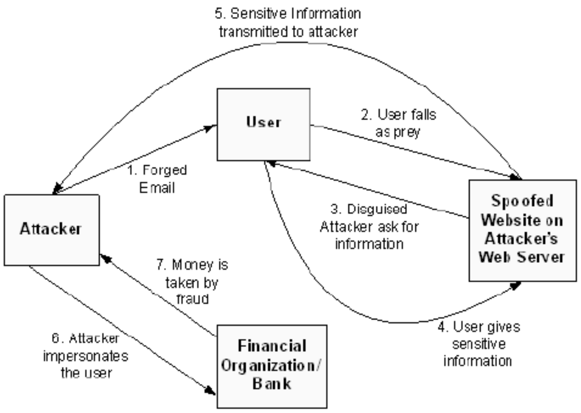

5. Sensitve Information transmitted to attacker
User
2. User falls as prey
1. Forged Email
Attacker
3. Disguised Attacker ask for information
Spoofed Website on Attacker's Web Server
7. Money is taken by fraud
6. Attacker impersonates the user
Financial Organization/ Bank
4. User gives sensitive information

Fig. 1: Phishing Process

Fig. 1 one shows the process of phishing and how cybercrimes are perpetuated using credit card information.

a. Adverse effect of indiscriminate internet use amongst children

There is a broad-spectrum of adversities associated with indiscriminate internet usage amongst children which ranges from health to social implications. Studies have shown that the circadian body function which controls the sleep-wake circle is affected by indiscriminate internet use amongst children. This is partly associated with long time spent online and addictive internet games. Depression has also been identified in recent times to be associated with social media usage amongst all population especially adolescents.

Stress is a health condition associated with undiscerning internet usage. Study found that using the internet for over 3 hours per day affects cortisol (stress inducing substance in the body) response in children leading to stress inducement [10]. Further research suggests that that adolescents who engage more with general media, use their phones more and have larger network sizes on Facebook may experience higher rises in cortisol after waking up, leading to higher stress level which can diminish metal response to a range of stimulus. Overeating, sedentary lifestyle and overweight are also commonly associated with indiscriminate internet use amongst children.

b. Risk Mitigation Approaches

Parental control plays a vital role in determining the scope and level of internet usage amongst children and adolescents. The terminology that adequately describes parental guidance towards safe internet usage is the mediation. [10] divided the parental mediation role into three types which are; active, technical and restrictive mediation. in active mediation, parents talk to children about internet risks and safer ways to use the internet, in technical monitoring, software and hardware restrictions are placed on the devices which limits/controls the level of access which the children have to the internet for instance, the firewall parents can set security policies are used to monitor and filter incoming and outgoing network traffic through a firewall, a network security device. A firewall is essentially the barrier that stands between a private internal network and the open internet at its most basic level. The basic function of a firewall is to let safe traffic in while blocking harmful traffic.

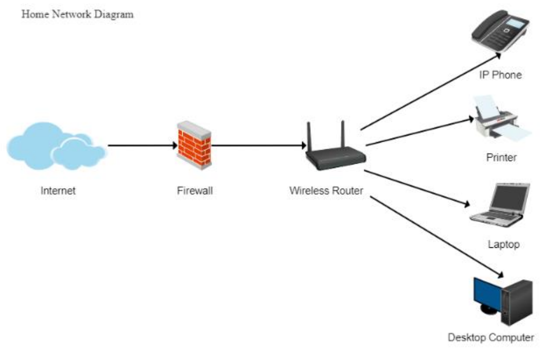
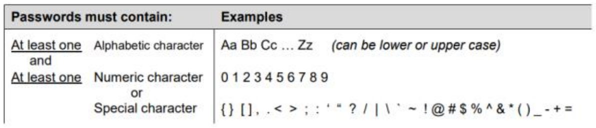


Fig 2: Firewall in the network architecture

Fig 2 shows the firewall layer in a typical home network architecture. while restrictions, involve setting rules that generally limit time use and/or limits or forbid access to certain types of content.

SOFTWARE TOOLS FOR PARENTAL CONTROL

There are several parental control approaches that can help prevent children from accessing unsafe and unsuitable content online. There are three suggested levels of parental control. These levels include network level, device level, and application control level. Network-level involves the use of networking devices like hubs and routers to ensure filtering and access control. Device-level control involves setting of authentication procedure like the two-way authentication and generally preventing access to devices which could be personal computers or smartphones, while application-level control involves setting proxies and limiting access to certain websites which are considered unsuitable for children. In some instances, setting of strong passwords on the devices is sufficient to totally cut off access. Below are suggested character combinations for strong password creation.



Passwords must contain:		Examples
At least one	Alphabetic character	Aa Bb Cc … Zz *(can be lower or upper case)*
and		
At least one	Numeric character	0 1 2 3 4 5 6 7 8 9
	or	
	Special character	{} [] , . < > ; : ' " ? / | \ ` ~ ! @ # $ % ^ & * ( ) _ - + =

Fig 3: Suggested Password Creation Table

IV. CONCLUSION

The Internet and its technological advancements paves way for improvement in the quality of life for everyone, however, some technologies pose some form of threat to the users. Children are particularly more vulnerable to the menace on the internet with severe consequences on both physical and mental health of the adversely affected child. Video game and social media are common amongst the indiscriminate use of internet amongst children and the negative effects include; alteration in sleep circle (circadian rhythm), stress, reduced productivity and depression amongst others. Parents should be actively involved in monitoring and guiding and where necessary, restricting access to certain internet content to protect children from the aforesaid adversities.

VII. REFERENCES

[1] Brody, J. (2015), Screen Addiction Is Taking a Toll on Children - The New York Times, https://well.blogs.nytimes.com/2015/07/06/screen-addiction-is-taking-a-toll-on children/?_r=0

[2] Hopkins, L., F. Brookes and J. Green (2013), "Books, bytes and brains: The implications of new knowledge for children's early literacy learning", Australasian journal of early childhood., Vol. 38/1, pp. 23-28,

[3] Chuck B. (2021), Global Thought Leader in Cybersecurity and Emerging Tech. https://www.forbes.com/sites/chuckbrooks/2021/04/12/3-key-cybersecurity-trends-to-know- for-2021-and-on-/?sh=55a322194978

[4] Geluvaraj B., Satwik P.M., Ashok Kumar T.A. (2019) The Future of Cybersecurity: Major Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cyberspace. In:Smys S., Bestak R., Chen JZ., Kotuliak I. (eds) International Conference on Computer Networks and Communication Technologies. Lecture Notes on Data Engineering and Communications Technologies, vol 15. Springer, Singapore.

[5] International Telecommunication Union (2016), "Measuring the Information Society Report"

[6] Lenhart, A. (2015), Teens, Social Media & Technology Overview 2015, Pew Research Center.http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/

[7] Duggan, M. and A. Smith (2014), Social Media Update 2013, Pew Research Center, http://www.pewinternet.org/2013/12/30/socia l-media-update-2013/.

[8] Finkelhor, D., Walsh, K., Jones, L., Mitchell, K. and Collier, A., 2021. Youth internet safety education: Aligning programs with the evidence base. Trauma, violence, & abuse, 22(5), pp.1233-1247.

[9] Alim, S., 2017. Cyberbullying in the world of teenagers and social media: A literature review

[10] Weinstein, A. and M. Lejoyeux (2015), "New developments on the neurobiological and pharmaco-genetic mechanisms underlying internet and videogame addiction", American Journal on Addictions, http://dx.doi.org/10.1111/aj