International Journal of Scientific Advances
ISSN: 2708-7972
Volume: 2 | Issue: 5 | Sep - Oct 2021 Available Online: www.ijscia.com
DOI: 10.51542/ijscia.v2i5.21

Digital Safety

Matthew N. O. Sadiku[1]*, Tolulope J. Ashaolu[2], Abayomi Ajayi-Majebi,[3] and Sarhan M. Musa[1]

[1]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX, USA

[2]College of Food Science, Southwest University, Beibei, Chongqing, P.R. China

[3]Department of Manufacturing Engineering, Central State University, Wilberforce, OH, USA

*Corresponding author details: Professor Matthew N. O. Sadiku; sadiku@ieee.org

ABSTRACT

Digital safety is a branch of cyber security that deals with people and the levels of online comfort, convenience, and privacy. It may be regarded as the act of staying safer online. This includes being aware of the risks associated with your online activity and avoiding being exposed to unwanted information, materials, or risks on the Internet that might harm one's devices. The Internet can be a risky place for children and their parents should have strategies for protecting them. This paper provides an introduction to digital security.

Keywords: digital safety; Internet safety; media safety; online safety; cyber safety; e-safety

INTRODUCTION

The digital technologies in general and the Internet in particular are changing the way we live, work, learn, and socialize. It is exciting to see the Internet making the world a better place. It has gradually moved beyond an educational and research and has been transformed into a commerce and healthcare juggernaut accessible to anyone anywhere anytime. The Internet has provided many important services accessible to anyone with a connection. There is almost no limit to what one can do on the Internet. The Internet is a wonderful place for learning, socializing, and entertainment, but it is also the home to certain risks, such as malware, spam, and phishing. It can pose dangers if precautions are not taken. Unsafe surfing can also lead to other threats.

Today, children use tablets, laptops, and smartphones at school and at home. They learn virtually, watch YouTube, play games, do research, communicate with teachers and other children. As a result, they have more information at their fingertips than any generation before. As the number of Internet users continues to grow around the world, governments, organizations, and parents are concerned about the online safety of children and teenagers. This has led to various regulations, like the Children's Online Privacy Protection Act (COPPA), to protect children when online.

WHAT IS DIGITAL SAFETY?

As people are eager to use mobile solutions that facilitate anywhere/anytime access, cyber criminals are constantly looking for ways to capitalize on this trend by taking advantage of unsecure wireless networks. Digital safety is learning how to safeguard your privacy and protect yourself from predators as we connect in this new digital age. Digital safety in variably known as Internet safety, media safety, online safety, e-safety, or cyber safety. It may include being aware of the risks associated with online activities and employing some strategies to prevent the risks or threats. Common threats to online safety include phishing, Internet scams, malware, cyberstalking, cyberbullying, online predators, and sextortion [1].

The following Internet safety rules are important in order to avoid getting into trouble online [2,3]:

(1) Protect Your Personal Information

Potential employers or customers may need to know about your expertise and how to get in touch with you. But they do not need to know your personal relationship and sensitive information. Any time you make a purchase online, realize that cybercriminals are most eager to get their hands on your personal information. Supply only information about credit card or bank account to sites that provide secure, encrypted connections. As shown in Figure 1, YAPPY is a useful acronym to help you remember the personal information you should not share online [4].

(2) Practice Safe Browsing

You should not visit dangerous neighborhoods online. Cybercriminals use lurid content as bait. By resisting the urge, you do not even give the hackers a chance. Be careful what you download. A top goal of cybercriminals is to trick you into downloading malware programs or apps that carry malware or try to steal information.

(3) Be Alert Online

It is essential to know whom you are dealing with online. Make sure your Internet connection and device are secure. You may use a secure VPN connection. If you are not using your electronic device for an extended period, turn it off or unplug it.

(4) Choose Strong Passwords

Passwords are the main defense against hackers. The problem with passwords is that people tend to choose easy ones to remember (such as "abcdefg" or "123456"), which are also easy for cyber thieves to guess. Select strong, complex, unique passwords that are harder for cybercriminals to demystify.

The password should be 15 characters long, mixing letters, numbers, and special characters.

(5) Be Careful What You Post

It is expedient for children and family members to know how much information is too much information and what can be posted online. Any comment or image you post online may stay there forever. Therefore, do not put anything online that you would not want your parent or spouse to see. To be Internet smart, you need to share with caution. As shown in Figure 2, before you post or text, THINK: Is it True, Helpful, Inspiring, Necessary, and Kind? [5].

(6) Keep Your Antivirus Program Up to Date

Your computer, laptop, smartphone, and tablet need to be protected. Protect these devices from virus malware and digital intrusion. Antivirus software protects your computer from viruses. Be sure to stay current with your operating system's updates and updates to applications you use. They provide a vital layer of security.

(7) Backup Data Regularly

Ransomware is popular among cybercriminals who can lock your computer. One way to combat the threat of ransomware is to backup your data regularly. Maintain a backup schedule so that you do not lose important files.

KEEPING YOUR CHILDREN SAFER

It is nearly impossible to connect with others online without talking to some people who are strangers. Some adults fear that children will use the Internet to connect with strangers. Banning your children from social media will take away a big component of their social life and a learning opportunity. It is better to have a strategy in place for Internet safety with the goal of helping them become a well-rounded person who can coexist with technology, not be ruled by it [6]. The following tips will help parents in keeping their kids safe online [7]:

- ***Remain positively engaged:*** Pay attention to and know the online environments your children use. Surf the web with them if necessary.
- ***Keep machine secure:*** Safety and security start with protecting all family computers with a security suite (anti-virus, anti-spyware, and firewall) that is set to update automatically.
- ***Review privacy settings:*** Look at the privacy settings available on social networking sites, smartphones, apps, and other social tools your children use.
- ***Teach critical thinking:*** Help your children identify safe, credible websites, and other digital content, and be cautious about clicking on, downloading, posting, and uploading content.
- ***Explain the implications:*** Help your children understand the public nature of the Internet and its risks and benefits. Remind them to limit sharing personal information with new friends.
- ***Empower your children to handle issues:*** Your children may deal with situations like bullying, unwanted contact or hurtful comments online.
- ***Encourage your children to be "digital leaders*"**:** Help ensure that they master the safety and security techniques of all technologies they use.
- ***Set boundaries*:** Put time limits on being online. Restrict social media access and email accounts, and set rules for emailing, texting, etc.

Teaching digital safety should be crucial component of today's classroom. It should the joint responsibility of parents and teachers, as shown in Figure 3 [8].

CONCLUSION

Through the Internet, we have unprecedented access to information, more than earlier generations. Today one can work, check bank balances, book travel, communicate with friends and family members, order books, and buy and sell online. As more and more children use the Internet in general and social media in particular, so do concerns about their online safety. Online safety or digital safety is becoming important, especially for children. Safety relates to a range of activities including online privacy, cyberbullying, exposure to violent content, contact with strangers online, and coarse language [9].

Everyone from the kindergarten to university should be made aware of their need for digital skills. Safer Internet Day is celebrated worldwide each year in February to raise awareness about internet safety. The World Economic Forum has led the Advancing Global Digital Content Safety initiative since September 2019. For more information about digital safety one should consult the books in [10,11].

REFERENCES

[1] "Internet safety", *Wikipedia*, the free encyclopedia https://en.wikipedia.org/wiki/Internet_safety

[2] "Top 10 Internet safety rules & what not to do online," https://usa.kaspersky.com/resource-center/preemptive-safety/top-10-internet-safety-rules-and-what-not-to-do-online

[3] "The cyber safety handbook," https://www.bmc.org/sites/default/files/About_Us/CyberSafteyHandbk-AARP.pdf

[4] K. Morris, "Teaching digital citizenship: 10 Internet safety tips for students (with posters)," March 2019, http://www.kathleenamorris.com/2019/03/12/internet-safety/

[5] S. Clegg, "THINK before you," www.joshshipp.com

[6] "Internet safety for teens: Practical tips & helpful resources," https://joshshipp.com/internet-safety-teens/

[7] "Raising digital citizens," https://staysafeonline.org/get-involved/at-home/raising-digital-citizens/

[8] "Digital safety and responsibility," https://www.fwisd.org/Page/24606,"

[9] G. C. Zilka, "Awareness of esafety and potential online dangers among children and teenagers," *Journal of Information Technology Education: Research,* vol. 16, 2017.

[10] J. R. Henrichsen, M. Betz, and J. M. Lisosky, *Building Digital Safety for Journalism: A Survey of Selected Issues.* UNESCO Publishing, 2015.

[11] N. Willard, Cyber *Savvy: Embracing Digital Safety and Civility*. Sage, 2011.

ABOUT THE AUTHORS

Matthew N.O. Sadiku is a professor emeritus in the Department of Electrical and Computer Engineering at Prairie View A&M University, Prairie View, Texas. He is the author of several books and papers. His areas of research interests include computational electromagnetics and computer networks. He is a fellow of IEEE.

Tolulope J. Ashaolu is the author of several papers and two books. His research interests include functional foods and food microbiology.

Abayomi Ajayi-Majebi is a professor in the Department of Manufacturing Engineering at Central State University in Wilberforce, Ohio. In 2015 he was honored by the White House as a Champion of Change for his significant contributions to the engineering education of minority students. He is a senior member of both the Society of Manufacturing Engineers and the American Society for Quality.

Sarhan M. Musa is a professor in the Department of Electrical and Computer Engineering at Prairie View A&M University, Prairie View, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Sprint and Boeing Welliver Fellow. His areas of research interests include computational electromagnetics and computer networks.

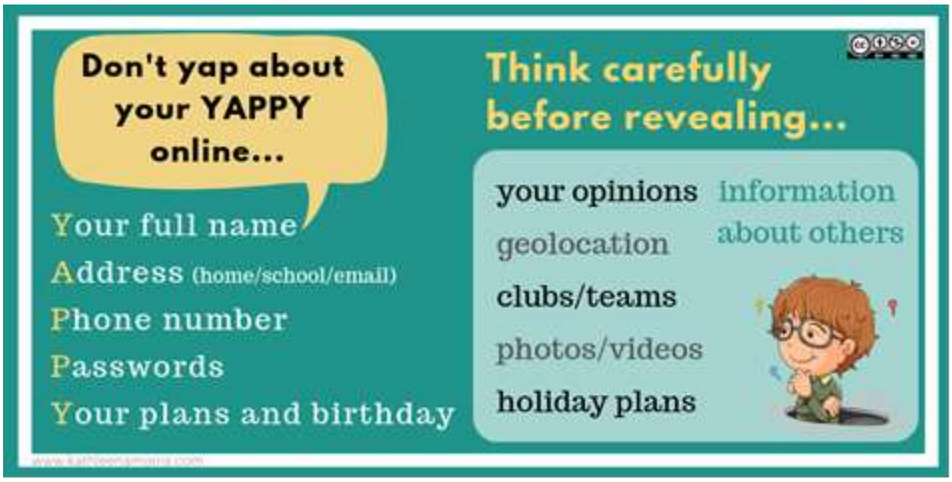

FIGURE 1: YAPPY is a useful acronym to help you remember the personal information you should not share online [4].

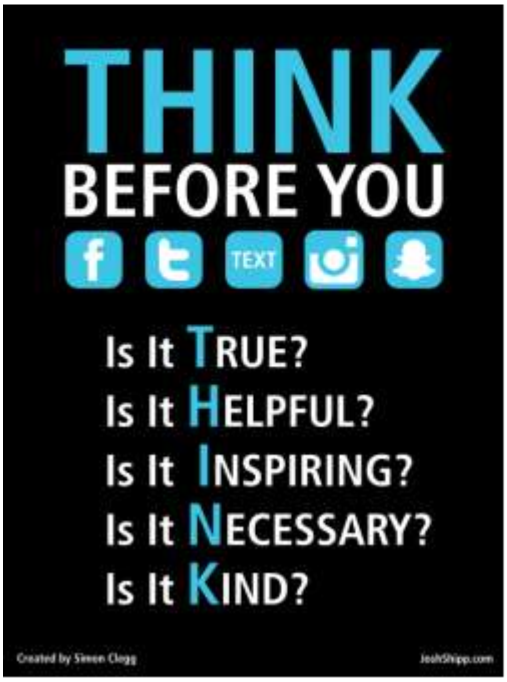

FIGURE 2: THINK before you post or text [5].

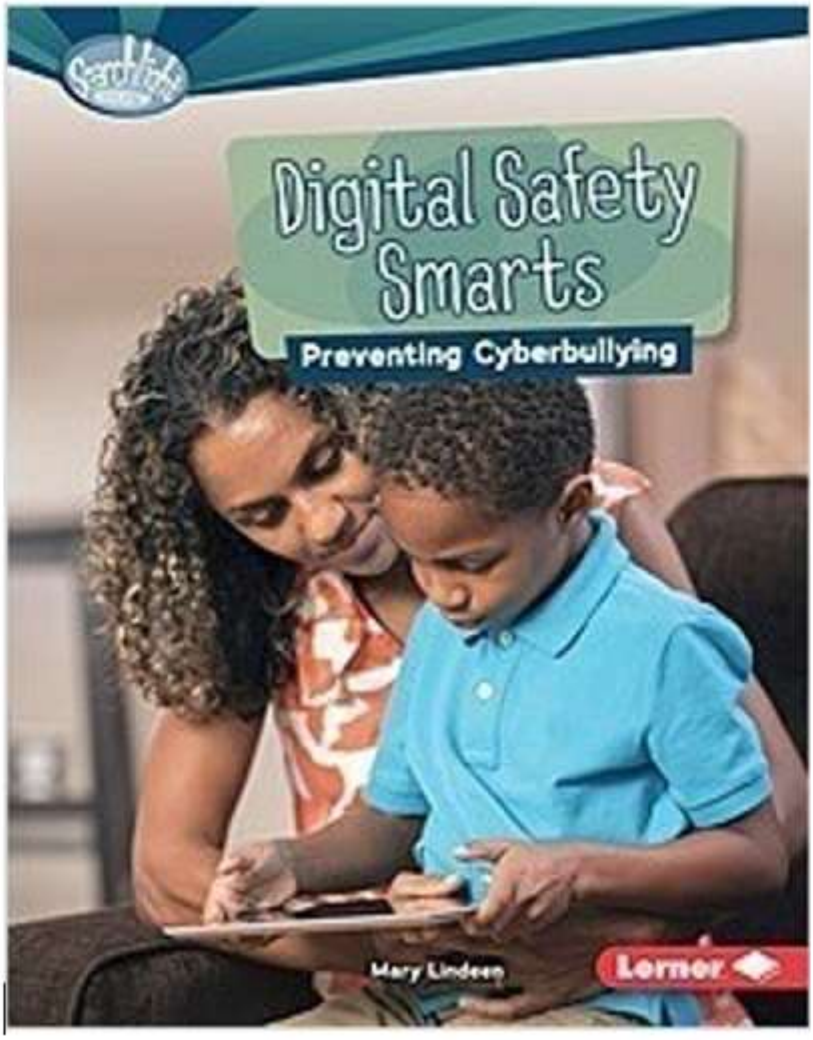

FIGURE 3: Parents and teachers are responsible for teaching digital safety [8].