Online Safety - The Risks Associated With Using the Internet, And the Strategies for Protecting Oneself Online

DR. AKEPE LINUS ENOBI
Digital Transformation, Cybersecurity, Forensic Investigation Strategist, IICFIP Continental Director for Africa

Abstract- ***The internet has revolutionized how people interact, learn, work, and consume content. It has made communication faster, easier, and more accessible, connecting people across the globe. However, as more people use the internet, it has also become a platform for criminal activities such as cyberbullying, identity theft, and phishing scams. Online safety refers to the measures taken to protect individuals and their information from online risks. This paper explores online safety, the risks associated with using the internet, and the strategies for protecting oneself online. The paper also looks at online safety challenges, and the various measures that individuals, organizations, and governments can take to ensure safe online interactions.***

Indexed Terms- ***Online Safety, emerging technologies, internet, protection, cyber threats, identity theft, scams, phishing attacks***

I. INTRODUCTION

The internet has revolutionized how people interact, learn, work, and consume content. It has made communication faster, easier, and more accessible, connecting people across the globe. However, as more people use the internet, it has also become a platform for criminal activities such as cyberbullying, identity theft, and phishing scams. Online safety refers to the measures taken to protect individuals and their information from online risks. This paper explores online safety, the risks associated with using the internet, and the strategies for protecting oneself online. The paper also looks at online safety challenges, and the various measures that individuals, organizations, and governments can take to ensure safe online interactions.

- Risks Associated with Using the Internet

1. Cyberbullying

Cyberbullying is a form of harassment that takes place online. It involves the use of technology to harass, intimidate, or embarrass an individual. Cyberbullying can take many forms, including sending hurtful messages, sharing private information, and posting embarrassing pictures or videos. It can have severe emotional and psychological effects on its victims, including anxiety, depression, and low self-esteem.

According to a study conducted by the Cyberbullying Research Center, over 36% of students in the United States have experienced cyberbullying at least once in their lifetime (Hinduja &Patchin, 2018). The prevalence of cyberbullying has increased due to the widespread use of social media platforms such as Facebook, Instagram, and Twitter. The anonymity and lack of face-to-face interaction make it easier for perpetrators to bully their victims.

2. Identity Theft

Identity theft occurs when a criminal steals an individual's personal information, such as their social security number, credit card details, or bank account information. The perpetrator can use this information to impersonate the victim and carry out fraudulent activities, such as making unauthorized purchases or opening new credit accounts.

According to a report by the Identity Theft Resource Center, there were over 1,000 data breaches in the United States in 2020, resulting in the exposure of over 300 million records (Identity Theft Resource Center, 2021). The increasing number of data breaches highlights the need for individuals to be more vigilant when sharing their personal information online.

3. Phishing Scams

Phishing is a type of online scam where criminals use emails or text messages to trick individuals into giving away their personal information, such as login credentials or credit card details. The perpetrators often use social engineering tactics to make their messages appear legitimate and convincing.

According to a report by the Anti-Phishing Working Group, there were over 241,000 unique phishing websites detected in the first quarter of 2021 (Anti-Phishing Working Group, 2021). The increasing number of phishing scams highlights the need for individuals to be more cautious when responding to unsolicited messages.

- Africa Children, Students & Online Safety

The internet can be a valuable resource for children and students in Africa, providing access to a wealth of information and educational opportunities. However, there are also several risks associated with using the internet, particularly for children and students who may be more vulnerable to online threats. Some of the main risks associated with using the internet for children and students in Africa include:

1. Exposure to inappropriate content: Children and students may come across inappropriate or harmful content online, such as violence, pornography, hate speech, and extremist content. This can have negative effects on their mental health and wellbeing, and may also lead to inappropriate behavior or attitudes.
2. Cyberbullying: Online bullying and harassment can occur through social media, messaging apps, and other online platforms, leading to emotional distress and even physical harm. This can be particularly harmful for children and students, who may be more susceptible to peer pressure and social exclusion.
3. Online predators: Children and students may be targeted by online predators, who use social media, chat rooms, and other online platforms to groom and exploit vulnerable individuals. This can lead to sexual exploitation, human trafficking, and other forms of abuse.
4. Cybersecurity threats: Cybercriminals may attempt to steal personal information, such as passwords, financial information, and identity documents, through phishing scams, malware, and other cyberattacks. This can lead to financial loss, identity theft, and other forms of harm.

- The African Union (AU) & Protection of Child Online

The African Union (AU) and various regional blocks in Africa have made efforts to protect children online. These efforts include the development of policies, laws, and initiatives aimed at safeguarding children from online abuse, exploitation, and other forms of harm.

Below some examples of the efforts made by the African Union and regional blocks in Africa to protect children online:

1. The African Union Convention on Cyber Security and Personal Data Protection: The convention was adopted in June 2014 and aims to promote cybersecurity and personal data protection in Africa. It recognizes the need to protect children online and calls for measures to prevent, detect and respond to cybercrime against children.
2. The East African Community (EAC) Child Online Protection Framework: The EAC developed a framework that provides guidance on how to protect children online. The framework includes provisions for legal and policy frameworks, education and awareness-raising, technical and procedural measures, and international cooperation.
3. The Southern African Development Community (SADC) Model Law on Child Marriage: The SADC developed a model law on child marriage that includes provisions on the prevention of child marriage and the protection of child brides. The law recognizes the role of the internet and social media in facilitating child marriage and calls for measures to prevent such practices.
4. The Economic Community of West African States (ECOWAS) Child Policy and Strategy: ECOWAS developed a policy and strategy that aims to promote the rights and welfare of children in West Africa. The policy recognizes the need to protect children online and calls for measures to prevent and respond to online abuse and exploitation.

In addition to these examples, various initiatives have been launched in Africa to promote online safety for children. For instance, the Global Partnership to End Violence Against Children, in collaboration with the African Child Policy Forum, launched the African Child Online Protection Initiative in 2017. The initiative aims to provide a platform for stakeholders to exchange best practices and develop strategies to protect children online.

- Government of the Republic of Cameroon & Child Online Protection

The government of Cameroon has taken several measures to protect children online, recognizing the potential risks and threats that children may face in the digital world. Here are some examples of what the government of Cameroon is doing to protect children online:

1. National Cybersecurity Strategy: In 2016, the government of Cameroon adopted a National Cybersecurity Strategy that includes measures to protect children online. The strategy aims to create a safe and secure cyber environment for all citizens, including children, and emphasizes the need to promote awareness and education on online safety.
2. National Committee on Internet Governance: The government of Cameroon has set up a National Committee on Internet Governance (NCIG) that is responsible for developing policies and regulations that protect children online. The NCIG works closely with other government agencies, civil society organizations, and the private sector to develop and implement effective measures to safeguard children in the digital space.
3. Child Online Protection Campaign: The government of Cameroon has launched a Child Online Protection Campaign that aims to raise awareness about the risks and threats that children may face online. The campaign includes a range of activities, such as public awareness-raising campaigns, educational programs for children and parents, and capacity-building initiatives for law enforcement and other stakeholders.
4. Child Online Protection Center: The government of Cameroon has set up a Child Online Protection Center that is responsible for receiving and processing complaints related to online child abuse and exploitation. The center works closely with law enforcement agencies to investigate and prosecute cases of online child abuse and exploitation.

- Civil Society`s Role in Promoting Online Safety

Civil society can play a vital role in promoting online safety for children by raising awareness, advocating for policies and regulations, and providing support and resources for children, parents, and educators. Here are some examples of how civil society organizations can contribute to online safety for children:

1. Awareness-raising campaigns: Civil society organizations can develop and implement campaigns to raise awareness among children, parents, and educators about online safety issues, such as cyberbullying, online grooming, and sexting. For example, the UK Safer Internet Centre runs an annual Safer Internet Day to raise awareness of online safety issues and promote positive online behavior.
2. Advocacy for policies and regulations: Civil society organizations can advocate for policies and regulations that protect children online. For example, in the United States, the National Center for Missing and Exploited Children (NCMEC) lobbies for legislation to protect children from online exploitation and provides resources for law enforcement, families, and educators.
3. Development of resources: Civil society organizations can develop and provide resources to support children, parents, and educators in promoting online safety. For example, the Australian eSafety Commissioner provides a range of resources, including safety advice, games, and educational materials, to help children, parents, and educators stay safe online.
4. Partnership with industry: Civil society organizations can partner with technology companies and online platforms to promote online safety for children. For example, the UK Safer Internet Centre works with technology companies to develop tools and resources to promote online safety for children.

Overall, civil society organizations play a crucial role in promoting online safety for children, and their

efforts can help ensure that children can benefit from the opportunities of the internet while staying safe from harm.

- Role of Churches

Churches can play a significant role in promoting children's safety online by raising awareness among parents and children about the potential risks and providing guidance on how to mitigate those risks. Here are some examples of how churches can help in children's safety online:

1. Educating parents and children: Churches can organize seminars and workshops for parents and children to educate them about the potential risks and ways to stay safe online. They can invite experts to speak on topics such as online grooming, cyberbullying, and online privacy.
2. Providing online safety resources: Churches can provide online safety resources such as websites, guides, and videos that parents and children can access to learn about online safety. For example, the Church of England has developed a digital charter that includes guidelines on online behavior and safety.
3. Monitoring online activities: Churches can monitor the online activities of children in their community to ensure they are safe. This can include setting up online safety software or tools that can alert parents and church leaders to potentially harmful content or activities.
4. Establishing safe online spaces: Churches can create safe online spaces for children to interact with each other, such as online forums or social media groups. These spaces can be moderated by church leaders to ensure that children are not exposed to harmful content or activities.

- Strategies for Protecting Oneself Online

1. Use Strong Passwords

Using strong passwords is one of the most effective ways of protecting oneself online. A strong password should be at least eight characters long and contain a combination of uppercase and lowercase letters, numbers, and symbols. It is also recommended that individuals use different passwords for different accounts to prevent a single data breach from compromising all their accounts.

2. Enable Two-Factor Authentication

Two-factor authentication is an additional security measure that requires individuals to provide two forms of identification before accessing their accounts. This can be a password and a fingerprint or a password and a code sent to their phone. Enabling two-factor authentication adds an extra layer of security to one's accounts, making it more difficult for hackers to gain access.

3. Use Antivirus Software

Antivirus software can help protect individuals from malware, viruses, and other online threats. It scans files and emails for potential threats, blocks suspicious websites, and alerts users when it detects potential threats. Installing antivirus software is essential for individuals who frequently download files or visit unfamiliar websites.

- Online Safety Challenges

Online safety challenges refer to the potential risks and dangers associated with using the internet and digital technologies. As technology continues to advance, so do the challenges related to online safety. Here are some examples and references of online safety challenges:

1. Cyberbullying: Cyberbullying is the use of digital communication tools such as social media, text messaging, and online gaming platforms to harass or bully another person. It can take the form of hurtful comments, rumors, and even threats. According to a survey conducted by the Cyberbullying Research Center, 37% of students in the US have experienced cyberbullying at some point.
2. Online Predators: Online predators are individuals who use the internet to target and exploit vulnerable individuals, usually children, for sexual or other predatory purposes. According to a report by the National Center for Missing and Exploited Children, there were over 13 million reports of child sexual exploitation material in 2019.
3. Identity Theft: Identity theft occurs when someone uses your personal information, such as your name, address, and social security number, without your permission. This can lead to financial losses and damage to your credit score. According to a report by the Federal Trade

Commission, there were over 1.3 million reports of identity theft in 2020.

4. Online Scams: Online scams are fraudulent schemes that are designed to steal money or personal information from unsuspecting individuals. They can take the form of fake websites, emails, and social media messages. According to a report by the Federal Bureau of Investigation, Americans lost over $4.2 billion to online scams in 2020.
5. Malware and Viruses: Malware and viruses are software programs designed to harm your computer or steal your personal information. They can be spread through email attachments, downloads, and infected websites. According to a report by AV-TEST, a leading independent IT security institute, there were over 10 million new malware samples in 2020.

These are just a few examples of the online safety challenges that individuals face in today's digital age. It is important to stay informed and take steps to protect yourself and your personal information online. Some ways to do this include using strong passwords, avoiding suspicious links and downloads, and regularly updating your software and antivirus programs.

- Challenges Faced by African Countries

Africa countries face a range of challenges concerning protection online. Some of the challenges include:

1. Lack of infrastructure: Many African countries lack the necessary infrastructure to protect online users. This includes weak cybersecurity systems, limited internet access, and inadequate data protection laws.

Example: In Nigeria, the lack of adequate cybersecurity measures has resulted in frequent cases of cybercrime, including phishing scams, identity theft, and financial fraud.

2. Limited awareness and education: Many Africans are not aware of the risks and threats associated with using the internet, and they lack the necessary knowledge to protect themselves online.

Example: In Kenya, many people fall prey to online scams, such as fraudulent investment schemes, due to limited awareness of online risks.

3. Limited legal frameworks: Many African countries lack comprehensive legal frameworks to protect online users, which makes it difficult to prosecute cyber criminals and enforce data protection regulations.

Example: In South Africa, data breaches and cyberattacks are common, but the country's legal framework for cybersecurity is still developing, making it difficult to hold perpetrators accountable.

4. Limited resources: Many African countries lack the resources and funding necessary to invest in cybersecurity infrastructure and training.

Example: In Ethiopia, the government has limited resources to invest in cybersecurity infrastructure, which has resulted in frequent cyberattacks and data breaches.

5. Political instability: Some African countries experience political instability and conflict, which can make it difficult to establish and enforce effective online protections.

Example: In Libya, ongoing conflict and political instability have resulted in limited cybersecurity measures and an increase in online threats such as hacking and cyber espionage.

Cameroon, like many other countries, faces numerous challenges in protecting children and students online. Some of the major challenges include:

1. Lack of awareness: Many parents and children are not aware of the risks associated with using the internet, such as cyberbullying, online grooming, and exposure to inappropriate content.
2. Limited access to internet safety tools: Many families and schools in Cameroon do not have access to internet safety tools, such as filtering and monitoring software, which can help protect children and students online.
3. Poor regulation of internet content: Cameroon does not have comprehensive laws to regulate the content that is available on the internet, which makes it difficult to prevent children from accessing harmful or inappropriate content.

4. Insufficient resources: The government and schools in Cameroon often lack the financial and technical resources needed to implement effective internet safety programs and initiatives.
5. Language barriers: Many internet safety resources and educational materials are only available in English or French, which can make it difficult for non-native speakers to access and understand them.
6. Lack of digital literacy skills: Many parents and teachers in Cameroon are not familiar with digital technologies and may not know how to teach children and students about internet safety.

To address these challenges, it is essential that the government, schools, and other organizations work together to raise awareness about the risks associated with using the internet and provide access to internet safety tools and resources. It is also important to invest in digital literacy training for parents and teachers, and to develop comprehensive regulations and policies to protect children and students online.

Overall, these challenges make it difficult for Africa countries to protect their citizens online, which can have significant economic and social consequences. Addressing these challenges requires investment in cybersecurity infrastructure, education and awareness, and legal frameworks that can effectively protect online users.

Measures to Stay Safe Online:

In today's digital age, safe online interactions have become increasingly important. Here are some measures that individuals, organizations, and governments can take to ensure safe online interactions:

1. Use strong and unique passwords: Use a combination of upper and lower case letters, numbers, and symbols to create strong and unique passwords. Avoid using the same password for multiple accounts.
2. Keep software up to date: Install updates and patches for software, operating systems, and web browsers regularly. This helps to protect against known vulnerabilities and exploits.
3. Use two-factor authentication: Enable two-factor authentication wherever possible, which requires a secondary form of identification, such as a code sent to a mobile device, to access an account.
4. Be cautious with email: Avoid clicking on links or downloading attachments from suspicious emails. Do not provide personal or sensitive information via email unless you are sure of the recipient's identity.
5. Use reputable antivirus software: Install reputable antivirus software on your computer to protect against malware and viruses.
6. Protect personal information: Be cautious about sharing personal information online, such as your full name, address, phone number, and date of birth. Only share personal information on trusted and secure websites.
7. Monitor financial accounts: Monitor your financial accounts regularly for suspicious activity and report any unauthorized charges immediately.
8. Use secure networks: Avoid using public Wi-Fi networks, which are often not secure, to access sensitive information.
9. Educate yourself: Stay informed about the latest scams and threats online. Learn how to recognize phishing attempts and other online scams.
10. Report suspicious activity: Report any suspicious activity or behavior online to the appropriate authorities, such as your internet service provider or local law enforcement.
11. Cybersecurity Policies: Organizations can develop and implement cybersecurity policies that address issues such as data protection, network security, and employee training.
12. Secure networks: Organizations and governments can secure their networks by using firewalls, virtual private networks (VPNs), and other security measures to protect against unauthorized access.
13. Encryption: Encryption can be used to protect sensitive data and communications from unauthorized access.
14. Data Backup: Regular backups of important data can help prevent data loss due to cyber-attacks or technical failures.
15. Incident Response Plan: Organizations and governments can develop and implement an incident response plan that outlines steps to take in the event of a cyber-attack or data breach.

By taking these measures, individuals, organizations, and governments can help to ensure safe online interactions and protect themselves and others from online threats.

- Resources Available to Help Ensure Online Safety

There are a variety of resources available to help ensure online safety. Here are some examples:

1. National Cyber Security Alliance (NCSA) - This organization provides resources and guidance on how to stay safe online, including tips for creating strong passwords, protecting personal information, and avoiding scams.
2. Federal Trade Commission (FTC) - The FTC has a website dedicated to providing information on online safety and privacy. They offer guidance on protecting your identity and avoiding scams, as well as resources for parents and educators.
3. Stay Safe Online - This website provides a wealth of information on online safety, including tips for protecting your personal information, securing your devices, and avoiding malware and viruses.
4. Common Sense Media - Common Sense Media provides resources and guidance on safe technology use for families and educators. They offer reviews and ratings of apps, games, and websites, as well as advice on how to manage screen time.
5. Google Safety Center - Google's Safety Center provides guidance on online safety and privacy, including tips for protecting your information online, securing your devices, and using Google's privacy tools.
6. McAfee - McAfee provides security software and services to help protect against online threats, including malware, viruses, and phishing attacks.
7. Norton LifeLock - Norton LifeLock provides a range of security products and services to help protect against online threats, including identity theft, malware, and phishing scams.
8. Cybersecurity and Infrastructure Security Agency (CISA) - CISA is a government agency that provides guidance and resources on cybersecurity and infrastructure security, including tips for staying safe online.

These are just a few examples of the many resources available to help ensure online safety. It's important to stay informed and take steps to protect yourself and your personal information whenever you use the internet.

REFERENCES

[1] UNESCO (2019). "Digital literacy and online safety in Africa: Opportunities and challenges." Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000367665

[2] Internet Watch Foundation (2021). "Online child sexual abuse in Africa." Retrieved from https://www.iwf.org.uk/what-we-do/online-child-sexual-abuse-in-africa

[3] United Nations Office on Drugs and Crime (2018). "Global Study on Sexual Exploitation of Children in Travel and Tourism 2018." Retrieved from https://www.unodc.org/documents/data-and-analysis/glotip/GLOTIP_2018_BOOK_web_small.pdf

[4] World Health Organization (2018). "Adolescent mental health in Africa." Retrieved from https://www.who.int/news-room/feature-stories/detail/adolescent-mental-health-in-africa

[5] African Union Convention on Cyber Security and Personal Data Protection. (2014). Retrieved from https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

[6] EAC Child Online Protection Framework. (2016). Retrieved from https://www.eac.int/document/eac-child-online-protection-framework

[7] SADC Model Law on Child Marriage. (2016). Retrieved from https://www.unicef.org/esaro/SA_Model_Law_on_Child_Marriage_FINAL_2016.pdf

[8] ECOWAS Child Policy and Strategy. (2008). Retrieved from https://www.refworld.org/docid/48f5fb6a2.html

[9] African Child Online Protection Initiative. (2017). Retrieved from https://www.end-violence.org/african-child-online-protection-initiative

[10] National Cybersecurity Strategy for Cameroon (2016): https://www.itu.int/dms_pub/itu-d/opb/pol/D-POL-DRCC-CM.01-2016-PDF-E.pdf

[11] Cameroon National Committee on Internet Governance: http://www.ncig.cm/

[12] Child Online Protection Campaign in Cameroon: https://www.itu.int/en/action/child-protection/Pages/Cameroon.aspx

[13] Child Online Protection Center in Cameroon: https://www.unicef.org/wca/stories/child-online-protection-centre-cameroon

[14] The Church of England's Digital Charter: https://www.churchofengland.org/resources/digital-labs/digital-charter

[15] The Child Exploitation and Online Protection command (CEOP) has produced a guide for parents and carers to keep their children safe online: https://www.thinkuknow.co.uk/parents/articles/keeping-your-under-fives-safe-online/

[16] The NSPCC has created an online safety guide for parents: https://www.nspcc.org.uk/keeping-children-safe/online-safety/