REPORT
CHILD ONLINE SAFETY IN THE ERA OF E-LEARNING

Introduction

There is little doubt that the Coronavirus (COVID-19) pandemic is affecting every aspect of our lives - from virtual classrooms to domestic violence, outright quarantines, etc. While countries are at different points in their COVID-19 infection rates, worldwide there are currently more than 1.2 billion children in 186 countries affected by school closures. As a result, education has changed dramatically, with the distinctive rise of e-learning, whereby teaching is undertaken remotely and on digital platforms.

According to (UNICEF), students are at increased risk of harm online because many of them are now taking classes online as well as socializing more online. Spending more time on virtual platforms can however leave children vulnerable to online sexual exploitation and grooming, as predators look to exploit the COVID-19 pandemic. A lack of face-to-face contact with friends and partners may lead to heightened risk-taking such as sending sexualized images, while increased and unstructured time online may expose children to potentially harmful and violent content as well as greater risk of cyberbullying. Research also suggests that online learning has been shown to increase retention of information, and take less time, meaning the changes coronavirus have caused might be here to stay.

Against this background, the Ovie Brume Foundation in partnership with Youth Empowerment Foundation and the Barack Obama American Corner held a webinar titled "Child Online Safety in the Era of E-Learning" on the 21st of May 2020. The session was moderated by Adeola Potts-Johnson, Head of Programs, Ovie Brume Foundation, and the speakers were Foluke Omoworare a UNICEF Consultant and Coordinator of Spotlight Initiative and Olamide Thompson-Odeneye, Convener, Child Online Safety NG. 90 people participated in the virtual class. Adeola Potts-Johnson welcomed participants and shared the objective of the webinar. This was followed by the introduction of the first speaker, Mrs. Foluke Omoworare.

The first presentation by Foluke Omoworare focused on "*advantages and risk/dangers of online learning, parent-child communication and practical tips in promoting online safety as well as the place of Child Rights in achieving online safety"*. The second presentation by Olamide Thompson-Odeneye focused more specifically on *"cyber security, the changes technology has brought, parental controls and antiviruses".*

Key Highlights of Foluke Omoworare's presentation

1. Child on-line safety means the act of protecting the identity and personal information of children below the age of 18 years who engage in personal development using various on-line mediums from unsolicited adults.
2. The role of parents in achieving online safety include ensuring that children are making profitable use of the internet as it relates to educational development and are not accessing age inappropriate sites or exposed to any form of abuse or harassment on the internet.

3. Parents however have to note that in achieving the afore mentioned point they do not infringe on the Child's Rights. (to learn, socialize and develop). Proper Child development does not take place when children live in fear. A child should respect their parents not fear them.
4. The e-learning risk children are exposed to can be broadly grouped into three: Content (what they are exposed to), Contact (who they interact with online) and Conduct (how they present themselves online). Thus, parents must safeguard their children from visiting inappropriate sites, ensure that they do not pose as older than their real age to exchange inappropriate messages and verify that they are not exposed to adults who can take advantage of their online presence to engage them in wrong messaging. This includes targeting them through chat rooms or social networking sites
5. Paedophiles often target children through chat rooms or social networking sites. They often "groom" (brain wash) them to excerpt information and disobey their parents.
6. With Paedophiles on the prowl, it is expedient for parents to have effective communication skills with their wards. Parents need to become knowledgeable about peculiarities and challenges associated with the Digital Generation.
7. Parents must understand and respect the individuality of the child. This is key so parents can learn how to separate Child Protection from Violation of Child's Rights.
8. Tips to protect children online:
    - Have regular child friendly discussions on internet safety, social networking, who to interact with and for what purpose. Parents should also dwell on dangers of interacting with strangers.
    - Specifically have regular discussions on cyber bullying, sexual harassment and unwanted solicitation as forms of child abuse that can impact negatively on their growth and development.
    - Put restrictions on children's devices.
    - Get adequate knowledge by being familiar with the online needs of children, internet sites they use and an understanding of how children use other devices like mobile phones and game consoles.
    - Continually monitor the child's internet activities by creating dedicated room for study where affordable. Re-organizing study areas for ease of monitoring (e.g. the positioning of desk so that you can observe what they are doing from an appreciable distance).
    - Ensure that the only search engine installed on the child's laptop are the verified safe search engine for kids e.g. kiddle.co
    - Equip children with age appropriate modules of Life Survival Skills (Assertiveness, Values, Decision Making, Goal Setting, Communication etc.). This will help them make right decisions when faced with negative peer influence.

The session ended on the note that, "a child is a child because they are innocent, naive, and have limited knowledge, thus it is the responsibility of parents to help them navigate through life. Being your child's best friend is the bedrock of child online safety and will promote effective and safe use of the internet by children.

Key Highlights of **Olamide Thompson-Odeneye Presentation**

1. Cyber safety is trying to be safe on the internet and is the knowledge of maximizing the user's personal safety and security risks to private information and property associated with using the internet, and the self-protection from computer crime in general.
2. Cyber safety also entails being responsible and respectful online, i.e. use of netiquette.
3. Cyber safety is important because it teaches a set of guidelines/rules/ideas to follow when interacting with people or websites on a computer, typically through the internet. This is essential as a person can easily end up having his/her identity stolen, lose money and files gone forever.
4. Cyber security awareness is a collective responsibility; it is imperative that this is understood as hackers use close ally to reach their targets.
5. The Cyber Security Intelligence Index, shows that 95% of all security incidents involve human error. This depicts that human beings are the strongest and weakest link in cyber security.
6. Having knowledge about cyber security does not make a person cyber aware but rather having the knowledge and putting it into practice.
7. General tips for Cyber Security:
    - Keep your personal information professional and limited, do not share unsolicited information particularly on social media.
    - Keep your privacy settings on your social media applications.
    - The use of the 2-factor authentication be used alongside safe browsing, be wary of free Wi-Fi.
    - Make sure your internet connection is secure, look for the padlock icon.
    - Be careful what you download.
    - Choose strong passwords, change them from time to time and use a phrase or alpha numeric combination.
    - Make online purchases from secure sites.
    - Be careful what you post, the internet never forgets. The rule before posting is Stop and Think before you Connect.
    - Be careful who you meet online. Do not take online relationship offline.
    - Keep all software up to date (anti-virus, operating systems etc). This is important as new viruses, malware e.t.c, are rolled out continually.
    - Don't get hooked by phishing scams, think before click, report and delete suspicious mails.
8. Technology is here to stay; thus, parents need to teach their children how to stay safe online despite the risks.
9. Risks that children face online:
    - Online Grooming
    - Cyber bullying
    - Sexting
    - Oversharing
    - Online Sexual Harassment
    - Identity theft
    - Inappropriate Content

- Malware
- Online Predators

10. Parental controls are features which may be included in digital television services, computer and video games, mobile devices and software that allow parents to restrict the access of content to their children. They are a great way to be proactive about a child's online safety and activities.
11. Parental controls function in various ways such as:
    - **Filtering and blocking:** this limit access to specific websites, words or images.
    - **Blocking outgoing content:** this prevents your children from sharing personal information online and via email.
    - **Limiting time** allows parents to set time limits for how long their children are online and the time of day they can access the internet.
    - **Monitoring tools** alert parents to their children's online activity without blocking access and can be used with or without the child's knowledge. Some software can record which websites a child has visited. Other programs display warning messages when children visit certain websites.
    - **Protection from malicious software** -- Antivirus protection not only protects computers from malware, it also offers parental controls that can help protect the child and computer. For example, Kaspersky safe kids,
12. Parental control often creates a false sense of security, as such parents still need to be vigilant on the activities of their children online and have internet discussion with the child.
13. Parents should note the following:
    - Don't block, technology is here to stay. Give your child an opportunity to harness the positive side on the internet.
    - Teach privacy—let them know what privacy is.
    - Collaborate with the Child. Get to know and understand what the child do on the internet.
    - Be the parent, protecting the child is key.
    - Set Rules and explain the reason for them.
    - Learn about the devices.
    - Be knowledgeable about age limitations for applications and games on the internet.
    - Communicate (be the trusted adult). Let the child have a sense of security with you as a parent.
14. 7 questions to help you start a conversation with your child about online safety:
    1) What apps/games are you using at the moment? Play the games with games with them
    2) Which websites do you enjoy using and why?
    3) How does this game /app work? Can I play?
    4) Do you have any online friends?
    5) Do you know where to go for help?
    6) Do you know what your personal information is?
    7) Do you know your limits?

Have a discussion with them, understand their language as the dialogue between a parent and a child is the most important factor for e-safety thus parents must cultivate an atmosphere for openness and acceptance.

15. Parents can adopt the SMART rules in communicating online safety with their wards:
    - Safe – do not give out your personal information online. Use a nickname for applications and games that require personal information.
    - Meet- teach children not to take online relationship offline. Discussion with online friends should take place ONLY with the supervision of a trusted adult.
    - Accept- Accept friend requests, emails, links e.t.c. from trusted and known sources only.
    - Reliable- verify every information; not all information on the internet is true.
    - Tell- tell your parent or trusted adult if someone or something makes you feel uncomfortable online.
    - Share with a heart, be polite to people online
16. To help your child stay safe online, work as a TEAM:
    - Talk a lot with the child.
    - Explore all technologies
    - Agree on limits
    - Manage the situation.

Q: What are NGOs in Nigeria doing to ensure the implementation of the Child Online Protection Act?
A: NGOs have been in discussion with the government in carrying out advocacy to ensure that the policy is being implemented.
Advocacy is ongoing and the involvement of Nigerian Communication Commission is aiding the process. In time past, online protection never involved children. Talks are now ongoing with countries where the law has been has passed to learn best practices. Filtration tools are also being put in place by service providers for family internet services.

Q: In this era of social media influencing where ideas and views are made popular by some 'online celebrity', regardless of the authenticity or moral standard of such views, how do parents and guardians deal with this?
A: Parents need to define and understand of who a celebrity is. A celebrity is that person who has paid their dues, learn the ropes of their career and have become outstanding. It is imperative for parents to let their children know who qualifies to be called a celebrity as not everyone who calls him/herself a celebrity is a celebrity.

Q: Can you recommend sites/apps as experts we can use to restrict our children's access to harmful sites?
A: The use of parental control features of antivirus is highly recommended. Parents should check if the antivirus they currently used has parental control and activate it. Parents can also download and use the free version of Karpaskey safe kids. The use of child friendly search engines such as Kidtopia, Kidsearch.com, Safe search kid. Is also important.

Q: Some children know more about devices than parents and may know how to circumvent some of these safety strategies we may want to deplore, how do we approach this?
A: Parents have to learn and understand how these devices work and operate them. In setting up parental control, it has to be done in a way that if tampered with, you can tell. However, the role of creating a sense of security with your child is important.

Q: What time duration would you recommend a child spends online - per day, per week?
A: the emergence of COVID-19 has brought a lot of changes to the educational sphere. This has necessitated a lot of online learning. It is therefore difficult to limit the timing a child can spend online, but you can only guide them. You can ask the child to draw up a time table to you give an idea of how long they will be online.

Q: Some children know more about devices than parents and may know how to circumvent some of these safety strategies we may want to deplore, how do we approach this?
A: Parents have to learn and understand how these devices work and operate them. In setting up parental control, it has to be done in a way that if tampered with you can tell. However, the role of creating a sense of security with your child is important.

Q: How do I activate parental control with my teenagers on Instagram and Facebook?
A: It depends on the age of the child. I do not advocate that children below the age of 16 be on social media and before they come online parents should have had the talk on cyber safety with their wards.

Q: How do we change the mindset of our children that the internet is not always the last resort to get information?
A: Continually have discussions with your children letting them know that the internet is also filled with junks. They need to know also that copying and pasting when carrying out assignments promotes lazy mentality approach in carrying out assigned tasks.

Q: How do we handle the issue of privacy of teenagers?
A: a child needs to understand how you want to help him/her. The challenge of role switching between adulthood and childhood must be taken into consideration whilst trying to help them. They do not have the psychological strength needed to navigate life challenges, so being your child's friend is key.

Q: Is there any support you can give students who cannot afford data as a lot of assignments and lessons notes are currently online?
A: Parents should reach out to the school authorities to know that there should be a limitation on number of assignments requiring students to go online because tech is here to stay. However, if the situation can be changed, have internet safety talk with the child.

Contributions to the discussion was also made by Chindima, Public and Private Development Center. According to her, setting up digital groundlines are good but parents have to be in charge. They can download

parental controls like Google Family Link. They are completely free and can be used offline, alongside antivirus and the use of child safe search engines.

Adeola Potts-Johnson thanked the speakers for an excellent session as well as thanked all attendees and admonished everyone to make use of the webinar information to ensure that every child is cyber safe, leaving no child behind. Olamide Thompson also added, that it takes a village to raise a child; keeping other children safe will ensure that your children are also safe.