



DIGITAL SAFETY



DIGITAL SAFETY, A CONCERN FOR ALL.

Digital safety can be referred to as the act of being “safe” digitally. Now, that sounds vague and shallow.

Let’s try again.

Digital safety, as the term implies, can be defined as the safe and sound environment in online medium. Basically, it is the application of human rights in the digital world.

Digital safety can also be referred to as internet safety, e-safety, online safety, or cyber safety. The term could vary but it points to one thing: staying free from harm electronically.

Do you need a reminder of how much harm can be done virtually? I bet you don’t.

Participation and involvement in the virtual world is not something you can successfully shield a child from even though it may be for his or her own good. This is because the world can use more hands to drag and pull them into the digital space.

Since we cannot effectively keep them away from the internet because of how much things have been integrated, we can however seek for ways to keep them safe on the space. This is essential.

It is a no-brainer how smart kids have become these days; how enlightened they are. This enlightenment is most of the time birthed by their innocent curiosity and the dispensation they are born into. They are so curious that they do not just want the surface "How’s", they also want the deep-rooted "Why’s", and will stop at nothing to get to the roots. You either let them in or they find someone who can.



Now, this is good. I mean it is good to let children explore the world but when the right systems that would curb the excesses are not in place, things are bound to go bad.

In today's digital age, children and teenagers are more connected than ever before. While technology has provided many benefits, such as instant communication and access to information, it has also created new risks. From cyberbullying to identity theft, trolling, stalking, verbal abuse, defamation, financial risks and so on. There are many potential dangers that we need to help our young people to become aware of.

Even before they pick up their first device, children in the modern world have a digital footprint. You must consider the information you are disseminating and to whom in order to ensure that your child's data is protected. Although it is an essential element of providing for your children and you inherently believe these institutions are reliable and secure, we tend to think little of disclosing our child's information to healthcare providers, hospitals, daycare centers, and schools. Sadly, cybercrime like data and identity theft can exploit even the most robust encryption software.

Let us explore some of the most common digital risks and provide tips for staying safe online.

CYBERBULLYING:

One of the most significant digital risks facing children and teenagers is cyberbullying. Cyberbullying is the use of technology, such as smartphones, computers, or social media, to harass, intimidate, or harm another person. It typically involves the repeated and deliberate use of electronic communication to bully, threaten, or humiliate someone. Cyberbullying can take many forms, including online harassment, spreading rumors, sharing embarrassing photos or videos, creating fake social media accounts to impersonate or harass someone and lots more.

To ensure our children are safe from cyberbullying, we should teach them how to be aware of these warnings signs:

Some of the signs that your little one is going through cyber bullying are:

1.Changes in online activity: When someone is bullied online, they may likely stop using social media or other online platforms. They may also change their behaviour on these platforms, for instance; deleting posts, deleting comments or acting strange each time they go online.

2. Mood changes: A victim of cyberbullying may become withdrawn, anxious, or depressed. They may also exhibit changes in behaviour, such as avoiding social situations, becoming more aggressive, or experiencing difficulty sleeping or eating.

3. Signs of distress: When under bully attack, they may show signs of distress, such as crying, yelling, or becoming angry.

As a parent, it will be important that you encourage your children to speak up if they or their friends are going through this experience. This will be a way of arming them ahead of time because to be forwarded is to be forearmed. You should also be on your guard to spot any or all of the above signs. Many times, children and teenagers are scared to speak up. So they tend to cover up and behave like all is well. Hence, it will take a third eye to spot this.

HOW TO REPORT CYBERBULLYING

1. Collect evidence: You can copy the URLs of the website or take screenshots of the material.
2. Report cyberbullying material to the social media service.
3. Report to a trusted adult
4. Block the person
5. Speak to someone you trust.

Kids should equally know that it is not right to bully others no matter the situation. Cyberbullying can have serious consequences on the victim some of which are depression, anxiety, social isolation and even suicide.

PRIVACY CONCERNS

Another digital risk that parents and teachers should be aware of is privacy concerns. Sharing personal information online can make it easier for hackers and identity thieves to gain access to your sensitive data. Also, oversharing personal details can also put them at risk of unwanted attention or stalking. Even young children as young as 10 use social media and at the very least disclose their name, age and sometimes a photo of themselves. By providing pictures and details about their location, favorite destinations, sports team, educational institution and social circle, their safety can be jeopardized.

To protect your children's privacy online, make sure to use strong passwords and avoid their sharing too much personal information on social media. Be cautious of suspicious messages or emails that ask for personal information and never share sensitive information, such as home address, social security numbers or credit card numbers, with any random person from the internet.



ONLINE SCAMS

Online scam is another digital risk that can be costly and dangerous. Scammers can deploy a range of tactics to trick both children and old adults into providing sensitive information or sometimes sending money. Common scams include phishing emails, fake social media profiles and fraudulent online purchases. Phishing is the act of attempting to get information such as usernames, passwords and credit card details by parading oneself as a trustworthy entity in an electronic communication. To avoid your children falling victim to online scams, you should encourage them to be cautious and skeptical of unsolicited messages or requests. They should always verify the identity of the sender and never give out personal or financial information unless they are sure of the authenticity of the request. If they cannot ascertain this, they should inform you, their parents or any trusted adult. If you suspect that they have fallen victim to a scam, report it to the appropriate authorities immediately. Cancel the request in terms of purchase or log them out from the device in use.

DEFAMATION AND HATE SPEECH

Defamation and hate speech are forms of online harassment that can have serious consequences. Defamation involves making false or damaging statements about someone that harm their reputation, while hate speech involves using derogatory language or slurs based on someone's race, religion, gender, or sexual orientation. To avoid engaging in defamation or hate speech, it is important that both teachers and patterns orientate our young ones to be respectful and mindful of others, even electronically. Rewarding such acts can also be a way of promoting it. They should avoid sharing false or misleading information as well as refrain from using derogatory language or slurs, no matter how common. If they see someone engaging in hate speech or defamation online, they should report it to the appropriate authorities.

RANSOMWARE ATTACKS

Ransomware is a form of malicious software that can encode your files and keep them in captivity until you provide a payment in exchange. Ransomware attacks can be expensive and devastating and can happen through infected email attachments, links or suspicious software downloads.



To avoid your children falling victim to ransomware attacks, make sure to keep their computer's software up-to-date and use reputable antivirus software. Be careful of suspicious emails or downloads, and instruct them to never open email attachments or click on links from unknown senders.



FINANCIAL RISK

FINANCIAL RISKS

It is important to bear in mind the financial risks associated with online transactions and purchases. Online scams, identity theft, and fraudulent transactions can all put your finances at risk.

Another danger in the digital age is online predators. These are people who use the internet to prey on innocent victims, often pretending to be someone they are not. They may try to get personal information from their victim or even try to meet them in person. To help protect children from online predators, Parents and teachers are to encourage them never to:

- Don't ever share personal information online.
- Never arrange to meet an online friend in person.
- Never hesitate to report any suspicious behaviour to an older person or to authorities.

ADDICTION AND SCREEN TIME

Another essential thing to consider is the risks associated with addiction and excessive screen time. Even adults sometimes struggle with this and so do children and teenagers.

Technology overuse can lead to negative physical and mental health outcomes, including disruption in their sleep patterns, eye strain, and even depression. It is important that you help them find a balance between using technology for learning or entertainment and engaging in real-world activities that promote physical and social well-being.

To avoid the risks of addiction and screen time, set boundaries for them around technology use and encourage healthy habits. Limit the amount of time spent on devices. This can be done by setting a standard app timer on their mobile device which when exhausted, the app freezes. Also, prioritize outdoor activities and face-to-face interactions and encourage open communication about technology use within your family or social circle.

Digital safety should be put in place to help children and teenagers to mitigate online risks and stay away from harm in the digital space. Going further into that, there are terms that you must be conversant with as a parent or teacher so you can effectively pass the same knowledge to the young ones. Let's look at some of the terms:

DIGITAL FOOTPRINT

This is the trail of data that is left behind after someone has interacted with a digital device or service. This data can include anything from the websites someone has visited to the emails they have sent.

DIGITAL REPUTATION

This is the public perception of someone's online persona. It can be shaped by a person's digital footprint as well as the content they share online. By all means, online security should be emphasized in such a way that they understand what they pose to risk if they do not take their digital safety seriously.

ISSUES OF MISINFORMATION AND DISINFORMATION

Some other risks that our naive kids are likely to fall victim of are:

MISINFORMATION

What is misinformation?

Misinformation is false or misleading information that is spread online. It can be intentionally or accidentally done, however, the consequences remain serious if it is believed by anyone.



DISINFORMATION

What is disinformation?

Disinformation is a false or misleading information that is deliberately spread online with the intention of influencing public opinion. It is usually used as a tool to manipulate people for political or financial gain.

In conclusion, issues of online safety should not be treated with a pinch of salt. It should be taken seriously. It should in fact be properly incorporated into our education system (curriculum) so that kids get grounded on these matters in time. Dedicating time to teaching these things in schools will make it easier for them to internalise, master and practice online safety

Digital safety is an important consideration for children and parents. By helping children stay aware of potential risks and take little steps to protect their personal information and privacy, they can each enjoy the benefits of technology while minimizing the potential dangers.

By promoting healthy technology habits and open communication, you can help your children navigate the complex digital landscape safely and responsibly. No one can do this better than you.

