CMSGu2021-01

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Cybersecurity Guideline for Youngsters

CERT-MU

National Computer Board
Mauritius

Version 1.0

January 2021

Issue No. 1

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this guideline is to provide essential information on online safety and privacy as well as encourage safe and smart decisions about online activity.

1.2 Audience

The target audience for this guideline is students, teachers, parents, grandparents, guardians and everyone else who deal with young people that are connected in some way or the other to the Internet.

1.3 Document Structure

This document is organised into the following sections:

Section 1 gives an outline of the document's content, the targeted audience and the document's structure.

Section 2 presents a background on how the online world affect youngsters.

Section 3 describes the online risks that youngsters are often exposed to.

Section 4 explains the precautions that youngsters can take to have a safe online experience.

Section 5 concludes the document.

2.0 Background

It is the right of every child to be taught how to stay safe online. Almost everyone is connected to the Internet these days, including the vast majority of teens and a growing number of young children. Whether by using a smartphone, accessing the web, watching a video, texting or playing a game, it is highly probable that you are connected.

In the new digital era, there are tremendous benefits to young people being online, however, there are also some device and network security risks, both digital and social. The digital kind involves apps and software that jeopardize the security of devices and the data on them. The social kind, often referred to as social engineering, is when people are tricked into putting their privacy and security at risk.

Moreover, kids and teens enjoy all that smartphones and tablets offer, from gaming to scheduling to photo-sharing to posting in social apps. Now almost everything that can be done on a computer can be done on a mobile device too, and apps are what deliver all this functionality.

The online world can also be a place of inappropriate conduct and content, where kids may feel anonymous. There are bullies, predators, hackers, and scammers that may pose a threat to children. These factors can make it challenging for parents to guide their children today on interacting with others through technology.

3.0 What are the risks?

The online world has many cyber risks for youngsters to recognize. The following are some of the cyber risks:

- **Cyberbullying** is bullying that happens online. It can happen in an email, a text message, an app, an online game, or on a social networking site.
- **Phishing/Identity Theft** is when a scam artist sends text, email, or pop-up messages in a browser to get people to share their personal information. They can then use that information to commit identity theft.
- **Sexting** is the sending or forwarding of sexually explicit photos, videos, or messages from a mobile phone. In addition to risking their reputations, friendships, and safety, this could be an illegal activity.
- **Social Networking** can help kids connect with family and friends, but it can invite danger if not used appropriately. Sharing too much information, posting pictures, videos or words can damage the reputation, hurt someone else, or invite a predator to contact the user. Once something is online, it may not easily be removed. Oversharing may be leveraged by online criminals to facilitate identity theft.

There are some security threats aimed specifically at kids or teens, but most are aimed at any potential victim, regardless of age. Sometimes they just involve websites or subjects that interest a lot of kids, such as social networking sites and other media-sharing services. As hard as it sometimes is for adults to know the difference between a legitimate offer and a scam, it can be even harder for children.

- **Kids love videos**

  Malicious links can turn up in popular video-sharing apps or sites such as TikTok and YouTube. Children should often be asked whether they have ever seen links that could take viewers to inappropriate or illegal content in other free apps or sites. They should also be asked what they do when they encounter them. If they were familiar with the scam they probably ignored them but these counterfeit links can be cleverly disguised. Ads, too, can either link kids to content that is not appropriate or scams and third-party sites that capture sensitive information. Young people need to be wary of “make a new friend” links, dating sites, and gossipy-sounding scams that look like invites from friends or tempt them to “find out who’s talking about you” or “…who has a crush on you.”

- **Kids often use family computers**

  Since most kids do not have credit cards, we might think that they are not vulnerable to financial crimes, but if children share a computer or device with parents, their online activities can affect all users, including any online shopping, banking or work parents do at home.

- **Kids can be big fans**

  Like a lot of adults, but sometimes with even more devotion or time, kids and teens follow and chat online about their favorite celebrities in all kinds of fields. There are lots of celebrity sites, and the ones operated by the celebrities themselves or entertainment news publishers are fine. But kids need to be extra wary of fan sites that turn up in search results but are not actually run by the celebrities and the people who cover them. It is not always easy to tell, but at least they are usually lower down in the search results.

- **Kids are social**

  There are social reasons why kids are hacked. One form of bullying is using a password a child has shared to break into his or her social media account and post embarrassing messages or images or use the account to spread spam or post links to malicious sites. Kids should be taught not to share passwords, even with their closest friends, and always to log out of accounts when they are finished using computers shared with other people, especially those used in public, such as at school or public libraries. Browsers and cookies remember passwords unless you use the browser's "private" or "incognito" mode or remember to delete your cookies and history.

- **Kids' IDs are valuable to thieves**

  It may be surprising that kids are sometimes the target of identity theft, where a criminal gets enough information about them (e.g., name, address, date of birth, identification number, phone number, etc.) to apply for credit or commit a crime in a child's name. Children are susceptible to this type of threat and do not find out that their identity's been compromised until much later, such as when they want to apply for student loans or credit cards.

- **Kids enjoy mobile apps**

  There are now hundreds of thousands of apps for smartphones and tablets, not all of them from reputable vendors. It is not uncommon for apps to record the user's location, unique identifier of the phone, and even such details as age and sex. Sometimes this information is necessary, such as a navigation app knowing your location or a social networking app knowing who your friends are, but some apps sell that information to businesses that can use it to market to a child or to create a profile of the phone user.

4.0 Protect Yourselves Online

4.1 General Safety Precautions

Talk to an adult you trust before you go online. For example, your parent or guardian.

An adult can talk to you about:

- what you can do online

- what you should not do online

- what websites or apps are safe to use
- what posts, photos and videos are safe to share

When you go online make sure an adult is around so you can

- Ask questions

- Get help

Talk to your parent or guardian before you

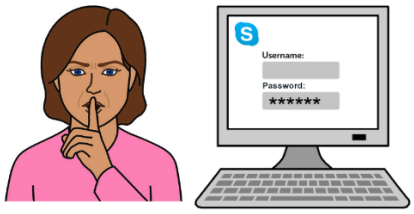
- Buy anything online

- Download or install something

– Download or install means you choose something online to save to your computer.

4.2 Online Privacy

You must keep your personal information safe online.



Personal information can be your

- address
- phone number
- password

In order to keep your personal information safe online, you must

- not let other people use your accounts and
- not give out personal information.

4.3 Making online friends

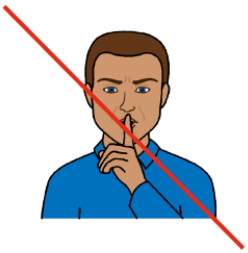
You might make a friend online.

It is safer not to meet them in person.

An online friend should

- talk to you in a nice way
- respect you
- not make you feel bad or uncomfortable

not ask you to do things you do not want to do. For example, keep a secret.

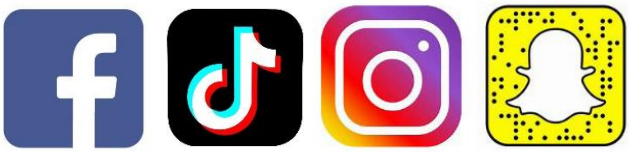


If an online friend asks you to do something you do not want to do

- tell an adult you trust

- report the person or message to the social media service

–A social media service might be Facebook, TikTok, Instagram or Snapchat.



- block the person to stop them from being able to contact you again

–Block means you stop the person from being able to contact you on the social media service.

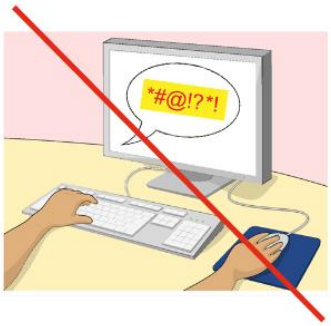
You might need to tell the police about your online friend

4.4 Viewing inappropriate contents

Talk to an adult if you see something online that you do not like or understand. For example

- photos or videos that are violent or sexual
- messages that are mean to you or tease you
- messages that make you uncomfortable

Do not answer messages that make you feel uncomfortable.



An adult can help you report bad messages to CERT-MU

CERT-MU can help you

- get support
- get rid of bad messages.

4.5 Security on mobile devices

- **Password-protect your phone**

  Almost all phones can be locked so that they require a simple numeric code, gesture, password or fingerprint to be functional. This will protect the information on your phone, prevent unauthorized calls and keep pranksters and people with bad intentions from using your phone to text or post embarrassing comments as if they are coming from you, a form of bullying. It also prevents "pocket-dialing" and it only takes a second or two to unlock your phone.

- **Check your phone's settings**

  Smartphones have privacy and security settings that control access to specific information such as which apps can access your contacts, calendar or location and to help you keep information from prying eyes. Look at the settings carefully, and change them if necessary.

- **Beware of in-app purchases**

  Before kids download apps, they should ensure they know what the app does, what information it collects and what it does with that information. While there are many apps that are free or legitimately charge for upgrades, additional content, special skills or advanced levels of games, there are also illegitimate apps that try to trick users into making purchases. Even if there are no tricks or outrageous charges, kids need to know when it is and is not OK for them to buy apps or make in-app purchases. Parents may work with them to establish a budget for what they are allowed to spend and, at least for younger kids, have a rule to check with a parent before any app is downloaded.

- **Look for legitimate apps**

  Sadly, there are cases of criminals distributing apps designed to steal your information. There is also the risk of a legitimate app being hacked by criminals. The solution is to download apps only from reputable marketplaces or app stores and, even there, read some reviews and ratings of the app you are interested in. Most kids will have heard of games and other apps from friends, which will help. If it is an app they have stumbled on, remind them to be cautious if there are only a few reviews or if it has not been downloaded by many people. Read the description carefully before installing it, and pay special attention to any disclosures about information that it collects. If there is no

information, be especially careful. If you doubt the legitimacy of an app you that have downloaded, delete it right away.

- **Use geolocation with care**

  This is important for all mobile users. Some location services, such as navigation systems or apps to help parents know where their kids are, can add to their safety, but not all apps need users' location. You can turn off geolocation for the entire phone but it often makes more sense to disable it for specific apps. So go over each app you use to see if it collects location information and, if you do not feel comfortable sharing that information, either turn off location for that app or, if that is not possible, delete the app.

5.0 Conclusion

Technology and the risks associated with it are constantly evolving, but a few things stay the same. When something great comes along, millions of people will want to use it and a small number of people are going to find ways to abuse it. In addition to the technical tools you and your family can employ to block cyber threats, by far the best defense is critical thinking, understanding when things are too good to be true or knowing to pause for a few seconds to consider the consequences of clicking on something, installing an app or entering a password or private information.

6.0 References

- https://www.connectsafely.org
- https://www.zdnet.com
- https://www2.ed.gov
- https://www.cisecurity.org
- https://www.esafety.gov.au