



CYBER SAFETY AWARENESS GUIDE

PART OF THE CYBER SAFETY AWARENESS TOOLKIT FOR LEARNERS



British
High Commission
Pretoria

UNISA



For further information visit:

<https://www.cybersecurityhub.gov.za/cyberawareness/>
<http://cyberaware.co.za>



Table of Contents

Foreword

BRITISH HIGH COMMISSION	1
DEPARTMENT OF COMMUNICATIONS AND DIGITAL TECHNOLOGIES: CYBERSECURITY HUB	2

UNIVERSITY OF SOUTH AFRICA	3
INTRODUCTION	4

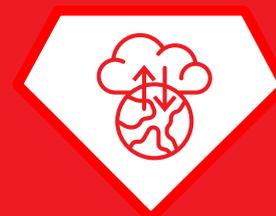


CYBER SAFETY IS KEY	5
---------------------	---



Cyber Safety Theme 1: A Trip Into Cyberspace

Introduction	6	Topic 1.1: Digital Footprint	8
Statistics / Interesting Facts	6	Topic 1.2: Cyber Risks and Threats	8
Advantages of Cyberspace	7	Topic 1.3: Online Privacy	8
Disadvantages of Cyberspace	7		



Cyber Safety Theme 2: Protecting People

Introduction	9	Topic 2.1: Cyberbullying	11
Statistics / Interesting Facts	9	Topic 2.2: Family Safety	11
Vulnerabilities of People	10	Topic 2.3: Communication, Respect and Ethics	11
Threat Actors	10		



Cyber Safety Theme 3: Securing Devices

Introduction	12	Topic 3.1: Technology Threats	14
Statistics / Interesting Facts	12	Topic 3.2: Mobile Devices	14
Positives of Devices	13	Topic 3.3: Malware Protection	14
Vulnerabilities of Devices	13		



Cyber Safety Theme 4: Smart Apps

Introduction	15	Topic 4.1: Social Media	17
Statistics / Interesting Facts	15	Topic 4.2: Safe Web Browsing	17
Positives of Applications	16	Topic 4.3: Gaming	17
Vulnerabilities of Applications	16		



Cyber Safety Theme 5: Useful Information

Introduction	18	Topic 5.1: Offensive and Inappropriate Content	20
Statistics / Interesting Facts	18	Topic 5.2: Cyber Scams	20
Positives of Information	19	Topic 5.3: Password Management	20
Vulnerabilities of Information	19		



Cyber Safety Awareness Pledge	21
-------------------------------	----

Cyber Safety Awareness Tips	22
-----------------------------	----



BRITISH HIGH COMMISSION



British
High Commission
Pretoria

The British Government is proud to have sponsored this initiative, which aims to increase cybersecurity awareness amongst learners who use digital platforms. We plan to continue consulting and partnering with government, private sector, educational institutions, subject matter experts, and civil society in South Africa to implement further cybersecurity initiatives like this.

The Cyber Safety and Awareness Toolkit was established to provide cyber safety and awareness education for learners, and to equip teachers with the ability to foster a cybersafety mindset and culture. We particularly aim to support underserved communities and schools which may lack the facilities to deliver cyber safety education.



Nigel Casey

British High Commissioner to
South Africa

This interactive toolkit has been developed in collaboration with the University of South Africa (UNISA) and the Department of Communications and Digital Technologies (DCDT). This partnership and the contributions made will catalyse digital inclusion and digital transformation.

The British High Commission would like to thank UNISA, the DCDT and the CyberSecurity Hub for their unwavering support during this process.



DEPARTMENT OF COMMUNICATIONS AND DIGITAL TECHNOLOGIES: CYBERSECURITY HUB



Pinky Kekana

Deputy Minister: Department of
Communications & Digital Technologies

The world of technology has given us so much, but none so much than in the era of a global pandemic, we're currently living through. It has allowed economies to remain somewhat active through people working from home, having team meetings, conducting sales pitches, eCommerce, home shopping and deliveries, and others. It has allowed children all over the world to still attend school, through online classrooms, for those who have access. Manufacturing of much needed PPE's have been possible, through technologies like 3D-printing. The reliance on digital technologies has become the norm for most people, across the world and in South Africa.

So, while innovation and emerging technologies has introduced us to a world of accessibility, convenience, and even greater variety, it unfortunately, also opens us up to the risk of being targeted by international and domestic cyber criminals. Cyber criminals have created syndicates and lucrative businesses from targeting private individuals, businesses both big and small, for a range of cybercrimes.

This creates a 'digital paradox', meaning that while governments and organisations can offer more services, more quickly than ever before, cybercrime has become a powerful countervailing force, that limits humanity's potential for positive innovation and growth, so far as technological advancement, is concerned. There have been an increasing number of attacks against national infrastructure, large-scale attacks against organisations, and data breaches of private citizen information.

Against the backdrop of the National Cybersecurity Policy Framework (NCPF), the Department established a Cybersecurity Hub in October 2015, creating a platform for South Africans to report cyber incidents and assist victims of cybercrime.

Part of the Hub's mandate is to implement a national Cybersecurity Awareness program, for citizens to be made cognisant of the threats and vulnerabilities of cyberspace, while they take advantage of the information age. Cybersecurity Awareness is a matter of behavioural change, and is a cultural challenge. As a national imperative, it demands a coordinated and holistic approach, as Cybersecurity Awareness initiatives must reach ALL residents of a country. In this context, the role of the private sector and academia must never be underestimated. To ensure this holistic approach and optimised reach, the Cybersecurity Hub was established as a central point, for the partnership between industry, government, and academia.

This ethos has been the basis of a new collaboration by the Department of Communications and Digital Technologies (through the Cybersecurity Hub), with the British High Commission, via the Foreign and Commonwealth Office (FCO), and the University of South Africa - to develop a series of cybersecurity awareness collateral, targeting students, educators, and parents.

We are extremely excited about this initiative, as we believe it will provide the guidance and practical knowledge for school learners, who are learning how to interact with the digital world around them. School learners are our biggest concern, as their increasing interaction, added to limited knowledge of the online world, and being generally oblivious to the risks and responsibilities of digital citizenship, makes them an easy target, and therefore our responsibility to them, to make them aware of the risks and threats they face.

The team has created a dynamic and multifaceted programme that I know will be welcomed by students, teachers, parents and caregivers alike, as it put them at the centre of this cybersecurity awareness programme.



Professor Elmarie Kritzing

University of South Africa

Technology is changing our world through a rapid and constant process by developing and providing Information Communication Technologies (ICT) and related devices to users around the globe. Many aspects of our lives have already been integrated with ICTs and ICT devices such as mobile phones, laptops, and tablets. Technology and ICT devices are becoming, smaller, vaster with greater technology capabilities. Technology is no longer a luxury but rather a necessity for many users.

We use ICTs and ICT devices to connect to cyberspace for communication, socialising and gathering information. Cyberspace is a global network that connects cyber users from around the world through a fast array of networks. Cyber users vary in age, religion, language and geographic location. More and more ICT devices are connected to cyberspace to form one global network of ICT networks, devices and cyber users.

Cyber users are becoming digital citizens in a cyber world with different rules, ethical considerations and even digital currencies. Each cyber user creates a digital footprint (for example, photos, text messages and search history) in cyberspace that cannot be changed or deleted. It is therefore critical that all cyber users understand the impact and consequences of their actions in cyberspace.

The advantages of cyberspace are vast and has benefits from the health to the education sector. ICT has provided cyber users with opportunities to instantly communicate with other cyber users across the globe, conduct online banking, work remotely, and buy goods from the comfort of your home. Other life-changing technologies include self-driving cars, 3D printing and online education. Technology has changed the way we think, act and live.

However, using technology and connecting to cyberspace also

has several disadvantages. Cyber risks and threats can lead to cybercrime (for example, identify theft, cyberbullying, and financial loss) and cyber users can be exploited and become victims to these cyber-attacks.

All cyber users (especially children and adolescents) must be made aware of cyber safety and how to ensure they understand the impact cyberspace can have on their actions, health, and emotional wellbeing. It is vital to understand that all cyber actions have consequences which may be to the benefit or detriment of the cyber user.

Cyberspace is not defined as good or bad but is defined on the actions of cyber users within cyberspace. It is therefore vital that all cyber users are made aware of how to act ethically in cyberspace as well as how to protect themselves and their information from other cyber users that have unethical and non-moral intentions.

The Cyber Safety Awareness Community Engagement project at the University of South Africa (UNISA) aims to assist and support cyber users (communities, school learners, teachers and parents) with the needed cyber safety awareness information to improve their cyber safety knowledge and skills to protect themselves and their information in cyberspace.

The aim is that all cyber users are safe, cyber safe.
www.cyberaware.co.za



An Introduction to This Guide

Information Communication Technology (ICT) has become an integral part of our daily lives. We use ICT devices for education, information gathering and work-related activities. ICT devices are becoming more accessible for all users due to increased availability and decrease in cost. Most of these devices have online connectivity, allowing the user to access cyberspace.

Welcome to the Cyber Safety Awareness Guide. This guide is aimed at general cyber users.

- This guide **aims** to create awareness for all cyber users regarding how to be cyber safe.
- The **key objective** of this guide is to improve general cyber users' knowledge and understanding of how to protect **themselves against cybercrime**.

Meet C², the cyber cadets on a mission to help you learn about how to be cyber safe. Each cadet represents an important cyber theme which you need to be aware of and learn about.

- Theme 1 (A Trip Into Cyberspace) we have **General Flame**. The leader of C² – She lost her eyesight in battle but gained amazing insight, by tapping into the vast knowledge banks in cyberspace.
- Theme 2 (Protecting People) we have **Professor Guardian**. She has a heart of gold. Although she has great empathy for people, she is tough on criminals and bullies that prey on the innocent.
- Theme 3 (Securing Devices) we have **Techno**. He is the expert on all things digital –he understands the inner workings of any device.
- Theme 4 (Smart Apps) we have **The Applicator**. He uses his vast influence on gaming and social media platforms, to unite people to support positive causes.
- Theme 5 (Useful Information) we have **Crypto**. She scans for sensitive information and helps to lock it down before the baddies can get their hands on it.



The guide is part of a cyber safety awareness toolkit designed to educate people about cyber safety, in different and exciting ways. You will have access to all the components to use as valuable tools to become cyber safe.

Online Platform



Workbooks



Word Searches



Videos



Posters



Cartoons



Games



For further information visit:

<https://www.cybersecurityhub.gov.za/cyberawareness/>

<http://cyberaware.co.za>



An Introduction Into Cyberspace

Cyberspace is the online world of computer networks and data banks, especially the Internet. It is also called the digital world, the world that you use when you use your phone, computer and any other device to go online.

As we use our devices for socialising, learning, gaming and many other things, we need to be aware of all the dangers in cyberspace to be able to protect ourselves and our devices. You have the right to be part of this awesome cyber world, without having to worry about all the risks (when you are exposed to danger) and threats (when you can be harmed by something)!

In this guide, you will learn about the most important ways to become cyber safe, because Cyber Safety is Key if we want to protect ourselves and all the people we care about.

Here are some of the advantages of being cyber safe:

By being aware you may avoid clicking on “free content” that lures you to open viruses, malware and ransomware.

I am safe; we are safe. Being cyber safe will protect you from a range of threat agents- online predators, bullies, criminals and the various tools and techniques they use. Practising good online habits benefit everyone at home, at school, at work and around the world.

Being cyber safe will protect you from getting viruses on your devices – an anti-virus is still very useful, so do not skip it. It will protect you from a lot of computer viruses.

Some of the risks and threats and what it means:

Threat agents - people or a group of people, that use cyberspace to hurt or steal from you (scam you), such as:

- **Online predators** - people that want to harm you in a sexual way.
- **Cyber criminals** - people that want to plant harmful software, like a virus, malware or ransomware, on your device to damage it or blackmail you.
- **Scammers** - people that want to steal money or information from you to use or sell.
- **Cyberbullies** - People who bully you through the use of electronic text via email, websites, social media or blogs.
- **Hackers** - A person or group of people who are skilled in the use of computer systems and may illegally gain access to private computer systems.
- **Unaware individual** - A person who is not aware that the action they are carrying out will result in the committing or support of a cyber-attack.

The guide will help you understand why cyber safety is so important. Here is how to use this guide:

- We will discuss the **5 themes** that will help you to be cyber safe, while having fun in the digital world.
- Each theme will first be introduced, and then the **3 topics** included within each theme will be discussed.
- **Your favourite cyber cadets** will be on hand to give you informational cyber awareness tips.
- Don't be concerned if you don't understand some of the **terminology** - we have made sure to give you fun explanations and meanings of the lingo used in cyberspace.

Themes and Topics

Theme 1: A Trip Into Cyberspace

Topic 1.1 - Digital Footprint

Topic 1.2 - Cyber Risks and Threats

Topic 1.3 – Online Privacy

Theme 2: Protecting People

Topic 2.1 - Cyberbullying

Topic 2.2 - Family Safety

Topic 2.3 – Communication, Respect and Ethics

Theme 3: Securing Devices

Topic 3.1 - Technology Threats

Topic 3.2 - Mobile Devices

Topic 3.3 – Malware Protection

Theme 4: Smart Apps

Topic 4.1 - Social Media

Topic 4.2 - Safe Web Browsing

Topic 4.3 – Gaming

Theme 5: Useful Information

Topic 5.1 - Offensive and Inappropriate Content

Topic 5.2 - Cyber Scams

Topic 5.3 – Password Management



Theme 1: A Trip into Cyberspace

It is important to understand your imprint in cyberspace.
With great power comes great responsibility.

For theme 1 we have **GENERAL FLAME** with the power to tap into the vast knowledge banks in cyberspace.

Introduction

Welcome to cyber safety theme one: A Trip into Cyberspace.

When referring to your imprint, this is your digital footprint. Your digital footprint is like the footprints you leave behind in the sand or a wet surface. However, this footprint is what you leave behind in cyberspace. Your digital footprint is made up of all the activities, actions and communications that you make online, which are traceable, as these activities are displayed online. Your digital footprint cannot be deleted.

A Trip into Cyberspace - Topics:	Topic	1.1	Digital Footprint
	Topic	1.2	Cyber Risks and Threats
	Topic	1.3	Online Privacy

Statistics/Interesting Facts

It is therefore important to know the facts about the digital world that we use every day:

DID YOU KNOW?

- Tim Berners-Lee invented the World Wide Web in 1989.
- The world wide web is so vast, that it is impossible to measure it's size!
- Every minute 20.8 million WhatsApp messages are sent around the world, and 220 000 tweets on Twitter.
- Social media use is almost double during Covid-19.



- 50% of all learners have experienced some form of cyberbullying.
- By 2022 around 1 billion people in Africa will have Internet access.
- There are about 13 842 attempted cyber-attacks in South Africa per day.
- 73% of South Africans have fallen victim to cybercrime already.

Cyber Safety Tips to be discussed in this lesson

Maintain a decent digital footprint

Realise that the content you create or share, may be stored in cyberspace forever.

Be aware of cyber risks and threats

You have the right to be safe online, but also remember to behave in a decent and responsible way.

Be wary of sharing your personal information

Information may be stolen and used by criminals or sold to marketers.



Theme 1: A Trip into Cyberspace

Advantages and Disadvantages of Cyberspace

We have so much information and technology at our fingertips!

We really live in a physical AND digital world!

The Internet and the digital world can be both awesome and risky. This is why our cyber safety has become just as important as our physical safety. Don't think for a second that cyber criminals are just fooling around or not very clever—they are highly organised, intelligent and very very skilful. Their sole purpose is to harm you in any way that they can!

Here are a few awesome and risky facts about using the Internet and having a digital footprint:

By having a digital footprint, we can...



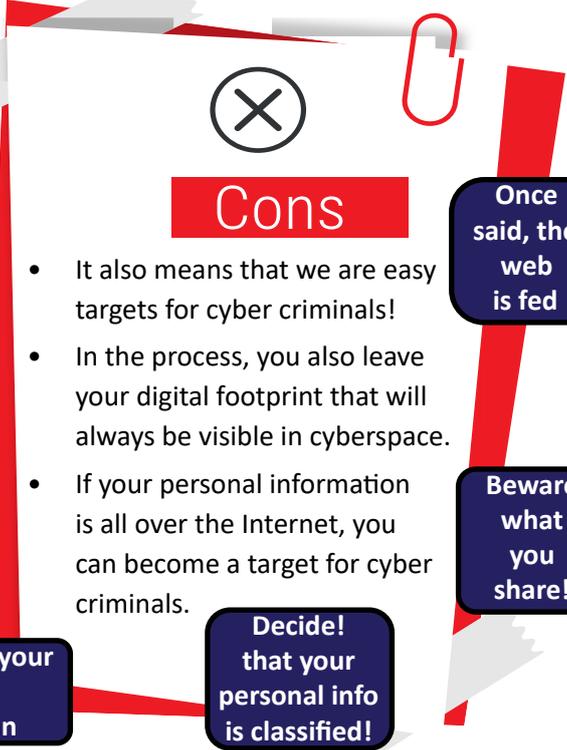
Pros

- Be active on the Internet and can research anything with just the click of a button!
- Easily connect with our friends and make new friends through their digital footprint.
- Learn so much about anyone; all you have to do is look them up online.

Cyberbullying? Report it, don't ignore it

But





Cons

- It also means that we are easy targets for cyber criminals!
- In the process, you also leave your digital footprint that will always be visible in cyberspace.
- If your personal information is all over the Internet, you can become a target for cyber criminals.

Once said, the web is fed

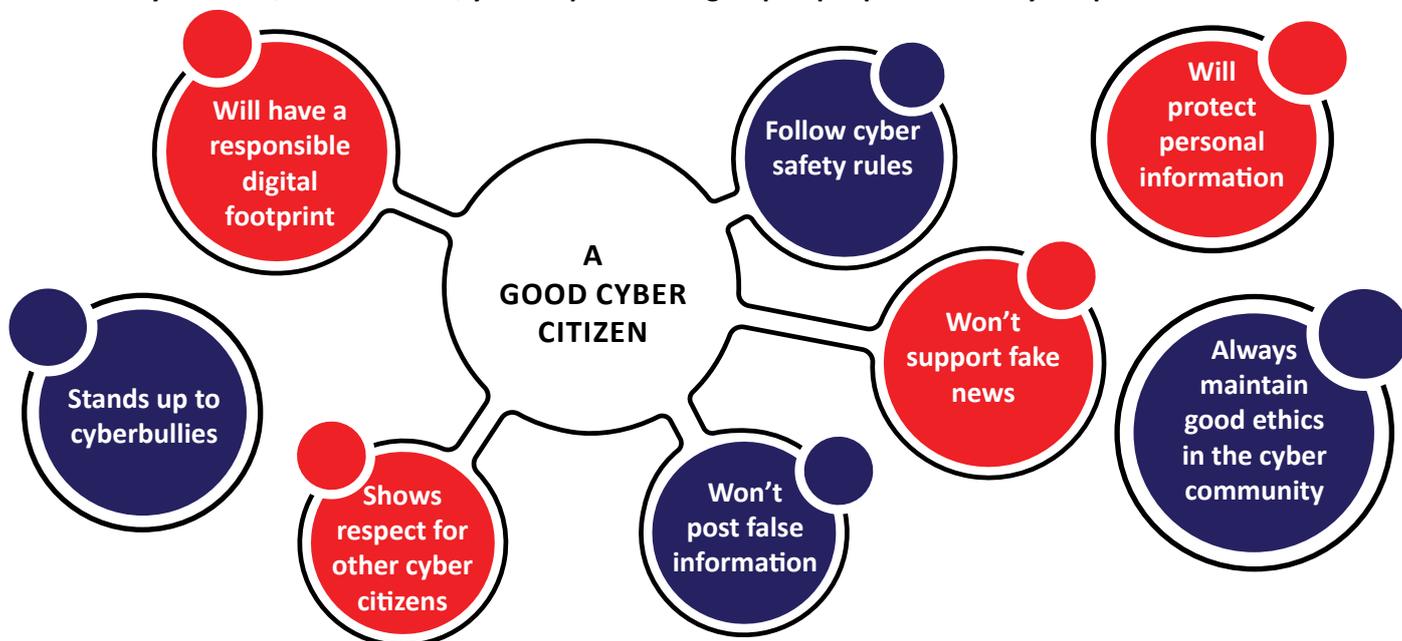
Beware what you share!

Decide! that your personal info is classified!

Be keen to keep your digital footprint clean

By being in cyberspace, you become a CYBER CITIZEN, because you are part of the digital or cyber community!

Cyber community is the online or virtual community. If you belong to a community, it means you belong to a group of people that you share your life with. This could be a physical community, like a church, school or the area that you live in, or in this case, you are part of the group of people that use cyberspace.





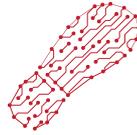
Theme 1: A Trip into Cyberspace

1.1 Digital Footprint

Did you know? Every time you go online on a device like a computer or your mobile phone, you leave a data-trace or imprint of your activity.

This trail about yourself and who you are, is called your

**DIGITAL
FOOTPRINT**



- Digital footprints are really useful, as it is the reason why you can connect with your friends on the Internet and even find new friends.
- You can get so much information on the Internet, with the click of one button!
- The trail you leave is always visible in cyberspace, which means that you can become a target for cyber criminals.

Simply put, it is everything on the Internet about you including:

- Social media profiles
- Images/ photos of you
- Any information or content posted by you on blogs and sites.

It is very important to be aware of your digital footprint, because if you do not keep it clean, strangers will get to know you without even meeting you. Make sure that your posts and your information can't be used against you.

1.2 Cyber Risks and Threats

Most people who use cyberspace do not know about the related risks and threats, which makes them targets for cyber criminals.

A risk is when someone or something is exposed to danger- if you are on the Internet, you are at risk to become a victim of crime. However, we cannot stop living or be afraid all the time, just because we are at risk of danger. By knowing the risks, and acting to protect ourselves, we can shape our own security in cyberspace.

- For instance: “free content” or “free downloads”, are usually just a trap to get the chance to insert viruses or malware on your device.

A threat is when there is a chance that you can be harmed in all sorts of ways. This usually is with the intention of hurting you and not by accident. Again, you are in charge. You can put yourself in a threatening situation by not following warnings and safety rules, or make sure that you become cyber smart!

- A good example of being at risk of an attack is if your privacy settings are on “public” for everyone to see. It is the perfect moment for cyber criminals to steal your personal information or make you a target for sexual predators.

You have the right to be safe online but also remember to behave responsibly.

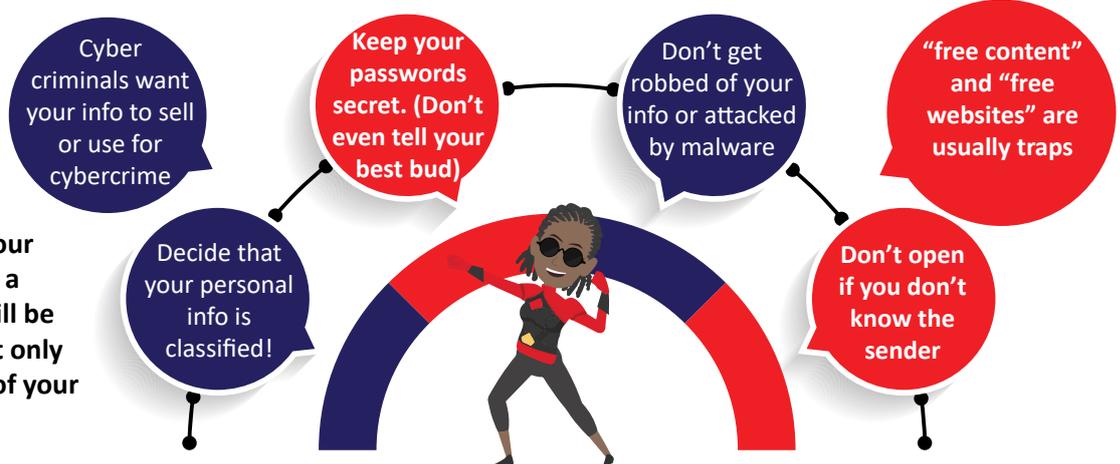


1.3 Online Privacy

Do you usually tell strangers your dreams and secrets and give them your personal information like your address and ID number? Of course not! So why would you do it online? In cyberspace, sharing is NOT caring!

If you put your personal information out there in cyberspace, of course, you will become the perfect target to cybercrime!

Protect yourself with your own “security key” (like a good password) that will be so difficult to hack, that only you will stay in charge of your safety.





Theme 2: Protecting People



Using cyberspace to communicate may expose you to many new vulnerabilities and threats from criminals, online predators or cyberbullies.

For theme 2 we have **PROFESSOR GUARDIAN** with the power to be tough on criminals and bullies that prey on the innocent.

Introduction

Welcome to cyber safety theme two: Protecting People. Communication is Key. This theme gives an overview of cyberbullying. How it is important to keep your family safe when in cyberspace, and how you should behave when online by following the guideline of communication, respect and ethics.

2.	Protecting People - Topics:	Topic	2.1	Cyberbullying
		Topic	2.2	Family Safety
		Topic	2.3	Communication, Respect and Ethics

Statistics/Interesting Facts

It is therefore important to know the facts about cyberbullying:

DID YOU KNOW?

- There is a law against bullying in South Africa, called "Protection from Harassment Act"
- More than 60% of learners surveyed in South Africa agreed that cyberbullying is worse than bullying face-to-face.
- 78% of parents believed that technology is a positive learning tool.



- More than 3.2 million learners are bullied annually in South Africa.
- Did you know that many of the learners that have great technical skills and know their way around the Internet are still unsure about how to behave and be safe on the Internet?
- Cyberbullying is one of the biggest causes of depression and suicide amongst learners.

Cyber Safety Tips to be discussed in this lesson

Report cyberbullying

If you are a victim of bullying, keep evidence of the bullying. Remember that you have rights as per the **2011 Harassment Act of SA**. Tell a trusted adult, don't ignore it, report it!

Be aware of both physical and cyber threats

By knowing about all the dangers and threats, you can keep yourself and your family safe.

Show respect to yourself and other people

Being online does not mean that you have the right to behave badly.





Theme 2: Protecting People

Vulnerabilities of People and Threat Actors

Vulnerabilities mean that you are at risk of being harmed. By having a digital footprint, you are visible in cyberspace and can easily become vulnerable or a target for threat agents.

In the introduction of the guide, we looked at why it is important to be safe in cyberspace and explained some of the threat agents in cyberspace.

- **Threat agents** are people that use cyberspace to hurt or steal from you.
- **Being cyber safe** will protect you from a range of threat agents such as online predators, bullies, criminals and the various tools and techniques they use. Practising good online habits benefit everyone at home, at school, at work and around the world.



- **Bullying** is when a person or a group of people, target someone to cause hurt and harm to the person. It is done on purpose and bullies use lots of ways and tools to target their victims.
- When the bullying happens online in cyberspace, it is called **cyberbullying**.

Don't be scared to speak up, if you are being bullied!

By not speaking up and communicating with your parents or caregivers about something which may be bothering you, you run the risk of being alone, scared and an easy target for cyberbullying. Here are a few reasons why good communication is important:



1

If you do not report cyberbullying, there is a higher chance of it happening continuously, with no end in sight.

2

Telling your caregiver or parent means they can open up an investigation to make sure that the cyberbully gets punished.

3

Your caregiver or parent can get in touch with the correct authorities and channels needed to report the cyberbullies.

4

It is your duty to speak up to not only stop the crime, but to spare other people of becoming victims too!

Sexual predators can be much more difficult to spot online than in real life. You might be thinking that it is a boy or girl your age that is keen to get to know you better, because they hang out on the same social sites as you and seem to have the same interests as you.

Be aware and stay alert by

- Not talking to people you don't know in real life and never agree to meet up with them.
- Being careful who you allow to follow you on Instagram - being popular on Instagram is a bit like being rich in Monopoly!
- Blocking anyone who makes you feel even the slightest bit uncomfortable online.
- Always telling a responsible adult if you are worried about a person that is sending unusual messages or requests.

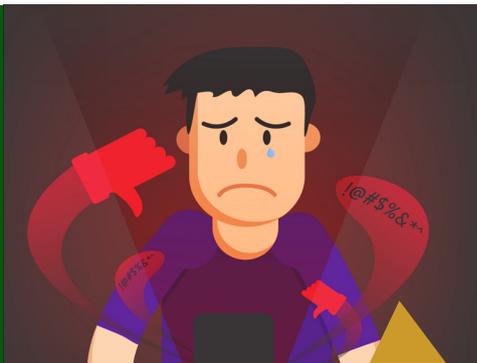


Theme 2: Protecting People

2.1 Cyberbullying

Do you know what kind of behaviour is seen as cyberbullying? Sometimes you might not even know that what you are doing, can be seen as bullying! Bullying can be:

- Picking on someone smaller and more vulnerable than you.
- Ongoing teasing and taunting to make someone ashamed or embarrassed.
- Playing mean online pranks or spreading lies about someone.
- Intimidating friends or fellow learners to stop being someone's friend, or to ignore someone completely.
- Sending hurtful or threatening messages, spreading fake information or news about a person and even their families.
- Making fun of someone's physical weaknesses or the way they look.
- Labelling someone to ruin their reputation.
- Forcing someone to do something illegal or dangerous.



Cyberbullies: cause harm through the form of electronic text via email, websites, social networking sites or blogs.

2.2 Family Safety

Your **digital footprint** can make not only you, but also your family vulnerable to criminals, if you are not aware of the threats, like:

- **Cybercriminals / Scammers:** These individuals carry out illegal scams and activities using the Internet.
- **Online predators:** Online predators are individuals who commit sexual abuse towards underage learners that begins or takes place on the Internet.
- **Hackers:** A person or group of people who are skilled in, or very good at using computer systems to get access to any private computer system.

You have the right to be safe online but also remember to behave responsibly.



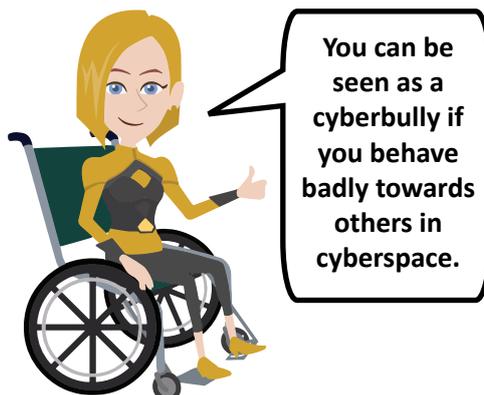
Don't be an **unaware individual**: A person who is not aware that the action they are carrying out, will help criminals to launch or support a cyber-attack. For instance, when your BFF sends you a link because they think it is a site full of cool free stuff, and it's actually a bad virus!

2.3 Communication, Respect and Ethics

If you protect yourself against all the risks and threats in cyberspace, you are keeping a responsible digital footprint. It's also important to show respect to your fellow cyber citizens. Here are some ways to keep good online ethics.

Respect is being aware of your own, or someone else's beliefs, feelings and needs and showing that you accept, value or consider these beliefs and good qualities of a person.

Ethics are a set of values or moral principles that you live by and how you conduct yourself, to be the best person you can be.



THINK

Before you post or share:

- T** Is it **True**
- H** Is it **Helpful**
- I** Is it **Inspiring**
- N** Is it **Newsworthy**
- K** Is it **Kind**



Theme 3: Securing Devices



Your devices need safekeeping too. Protect them against threats and vulnerabilities.

For theme 3 we have **TECHNO**: with the power to understand the inner workings of any device.

Introduction

Welcome to cyber safety theme three: Securing Devices. We are truly living in a world where new technology hits the world market almost daily! Besides cell phones, laptops, desktop computers and tablets, we now have access to 3D printers, gaming consoles, tracking devices and a range of robotic gadgets. Accessing information and communicating is so much easier and instantly. We are going to look at the impact that technology has on our lives, and why it is so important to keep our devices safe and protected.

3.	Securing Devices - Topics:	Topic	3.1	Technology Threats
		Topic	3.2	Mobile Devices
		Topic	3.3	Malware Protection

Statistics/Interesting Facts

It is therefore important to know the facts about devices:

DID YOU KNOW?

- Did you know that there is a hacker attack every 39 seconds?
- There are 5.16 billion unique mobile phone users in the world today, and counting.
- More than 25% of cyber-attacks involve malware or malicious software.
- Cell phones are such a big part of our lives that there's now a phobia called 'Nomophobia', which is the fear of being without your cell phone (or phone signal).
- The first mobile phone was made in 1974 by Martin Cooper and it weighed 1 kg.



- South Africa received the first cell phone in 1994.
- The word 'cell phone' comes from the way the device operates. Towers serve areas with signal and are divided up into cells.
- The average person unlocks their phone 110 times every day.
- There are more cell phones in South Africa than there are taxis, TVs and radios combined!
- The first electronic computer ENIAC weighed more than 27 tons and took up 1800 square feet.
- Only about 10% of the world's currency is physical money, the rest only exists on computers.

Cyber Safety Tips to be discussed in this lesson

Educate each other

Help one another by passing on info on new apps, sites, technologies, and threats – always share and communicate.

Keep your mobile devices safe and secure

Make sure that your devices are secured by a passcode or password. Also ensure that your sensitive personal information can be remotely deleted.

Protect against malware

Update all apps and install reputable anti-malware software on all your devices.





Theme 3: Securing Devices

Positives and Vulnerabilities of Devices

In today's world, we rely on our devices to communicate, learn, socialise, shop and store our information. This is all great, and so much faster to achieve a lot of things in our daily lives. BUT... it can also put us in danger by making us targets for cybercrime- and so there are just as many disadvantages to technology, and more specifically, devices.

Here are a few of the advantages and disadvantages:

Pros

- Devices help you access the Internet and share useful material for learning, school, and socialising.
- Access to mobile devices is becoming easier and less expensive.
- Mobile phones let us do lots of things like taking pictures, recording videos, reading, and downloading apps.

But

Cons

- The Internet is full of threats and possesses a variety of risks, including scams and the spread of fake news and lies. You can become a target or be at risk, the minute you switch on your device.
- Even your old devices and other electronics are vulnerable to thieves, who want to extract or steal valuable student and staff data.
- Mobile devices with location services enabled can be tracked by criminals.

Even if a device is old, cyber criminals see it as gold

Don't just believe information, it could be a false explanation

Beware of all the scams out there!

Disable location settings!

Beware what you share!

Make sure that your devices are protected!



Install anti-malware



Enable lock icons



Disable location services to avoid being tracked



Delete apps you do not use



Make sure that your setting is "private", not "public"

Remember photos store your location. If you post photos, people can see where the photo was taken.



Theme 3: Securing Devices

3.1 Technology Threats

New apps and software appear all the time, from finding your phone, to making a video, ordering food or transport and of course, all the social media apps!

With all the wonderful technology at our fingertips, we are now also faced with all the risks and threats that come with it. Every time we go online in cyberspace, we are exposed to cyber criminals, waiting to attack. We know that cyber criminals are smart and well organised; after all, they usually have the very best technology to use against us!

So, we need to be aware of technology threats and how to protect and secure our devices.

- Keep up to date with the latest technology, and share it with your friends. Communication is important to warn each other of the latest ways that cyber criminals use to try and harm you and your devices.
- Don't share important information and make sure that your settings are not on "Public" when using technology.

3.2 Mobile Devices

Mobile devices are a very important part of every action we take during a day. If we don't take care of our devices, it ...

- Can be stolen or lost. If you cannot wipe your information remotely, your information can be used for cybercrime.
- "Old" devices can be used to access information. Cell phones are becoming cheaper, which means that you might have old devices lying around. Make sure to transfer or save all your information, before you get rid of the device, sell it second hand or pass it on to a friend.
- Can make you a target. Disable location settings so that you do not become a victim of stalking and always use the lock screen function on your device.

Again,
it is up to
you to be
responsible
and to look
after your
own safety,
by securing
all your
devices!



3.3 Malware Protection

Malware, short for **malicious software**, is software that is used to harm or disable your devices, such as viruses, ransomware and worms.

Cyberspace is not always safe. Not all websites and apps are legit. Some websites and apps are fake, and it is just a way to get you to infect your device with viruses, steal information and disable your device. To install and have anti-malware software and a good firewall on your computer and other devices, is not a "nice-to-have". It is a "MUST HAVE"!

If you do have good, reputable anti-malware protection, make sure that you keep it updated. Sometimes we are so excited when we try a new device, that we forget to pay attention to notifications or messages that request you to update to the latest software protection.

Communicate with your parents and caregivers so that they are aware of your online activity and always ask their permission before you download. It is all worth it, so that you can stay safe while having fun in cyberspace!



Theme 4: Smart Apps



Whether you use applications for socialising or gaming, it is important to understand how to use them safely.

For theme 4 we have **THE APPLICATOR** with the power to influence gaming and social media platforms to unite people to support positive causes.

4. Smart Apps - Topics:

Topic	4.1	Social Media
Topic	4.2	Safe Web Browsing
Topic	4.3	Gaming

Introduction

Welcome to theme four: Smart Apps. An application is also referred to as an app. An App is a type of software that may be downloaded onto a device, and some may be malicious.

There are millions of apps out there to choose from, and we are using apps for different aspects of our lives. What makes technology and apps so amazing, is that it is in real-time - instant information, games, movie channels and much more at the click of a button! Smart apps have really changed how we study, socialise and communicate. This is why you need to be aware of all the ways that you might be exploited (used) while being online.

Statistics/Interesting Facts

First, some interesting facts about apps:

DID YOU KNOW?

- Did you know that there are 36,54 million Internet users in South Africa?
- The most popular device for using the Internet by learners in South Africa is a mobile phone.
- On average, South Africans spend 2 hours and 48 minutes a day on social media.



- Did you know that by keeping your browser software up to date you are practising safe web browsing?
- Did you know that in 2018 research showed that there were more than 11 million gamers in South Africa?
- The global gaming market is estimated to be worth +-R2600 billion.

Cyber Safety Tips to be discussed in this lesson

Understand social media

There are loads of social media platforms for all tastes – good and bad! Choose wisely.

Be safe when web browsing

Only use secure and legit websites with a good reputation for online browsing. Ensure that there is a lock icon at the top of your browser.

Take precaution on all apps and gaming platforms

Use a vague username and never share personal information or your address with people you meet online.



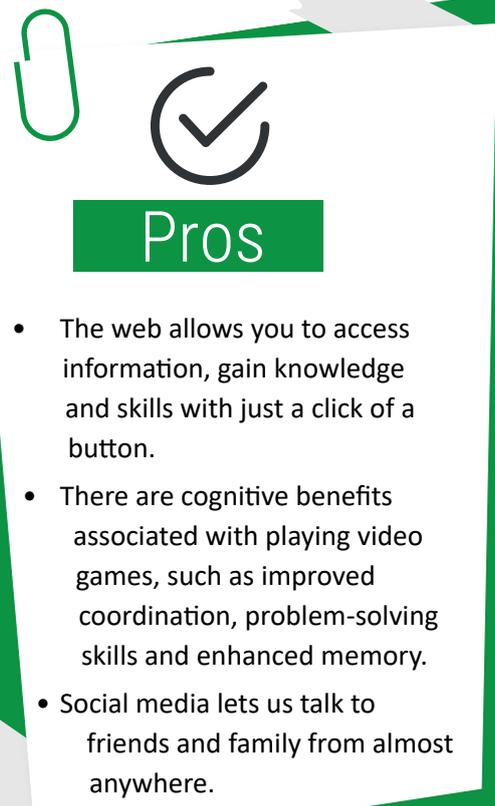


Theme 4: Smart Apps

Positives and Vulnerabilities of Apps

Most learners know their way around cyberspace and have great skills when using technology. People all over the world benefit from all the new technology and cyberspace. Most parents agree that technology is a fact of life for the youth and that it can be used for learning, socialising and discovering amazing information about the world we live in.

Let's look at some of the advantages and disadvantages of apps:

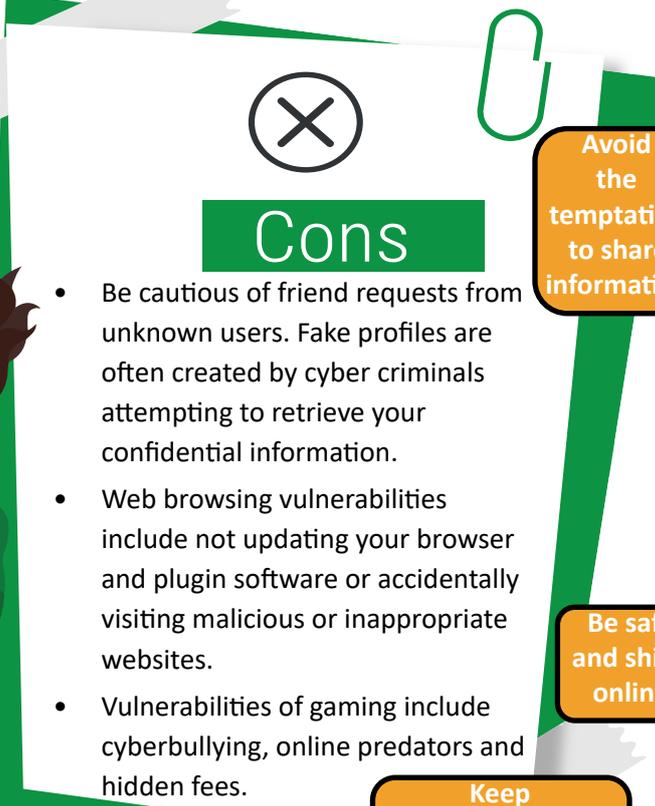


Pros

- The web allows you to access information, gain knowledge and skills with just a click of a button.
- There are cognitive benefits associated with playing video games, such as improved coordination, problem-solving skills and enhanced memory.
- Social media lets us talk to friends and family from almost anywhere.

But





Cons

- Be cautious of friend requests from unknown users. Fake profiles are often created by cyber criminals attempting to retrieve your confidential information.
- Web browsing vulnerabilities include not updating your browser and plugin software or accidentally visiting malicious or inappropriate websites.
- Vulnerabilities of gaming include cyberbullying, online predators and hidden fees.

Downloading? It's your parent's decision to give permission!

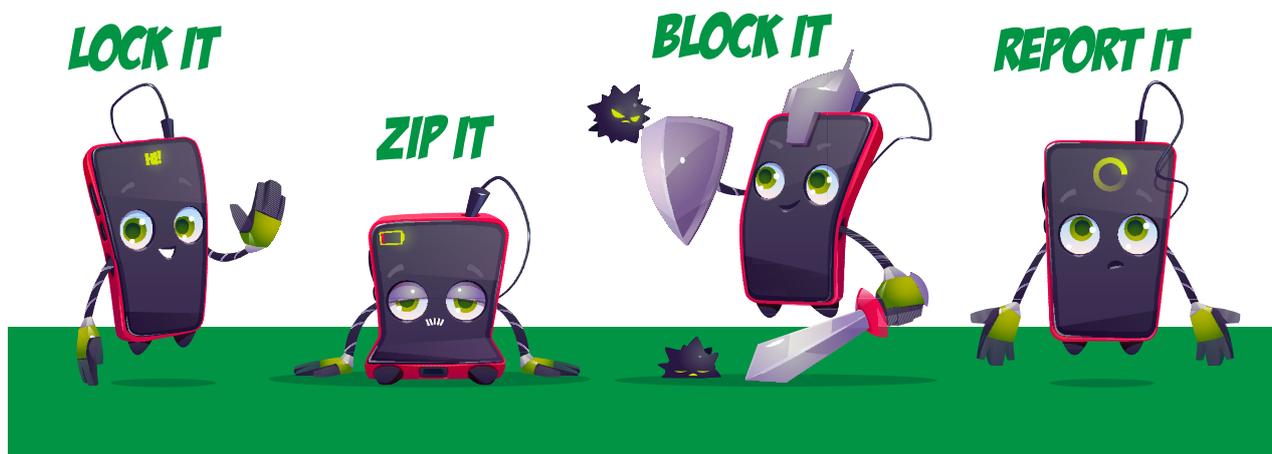
Communication is key!

Keep anti-malware and your firewall up to date

Avoid the temptation to share information

Be safe and shine online

Remember to be techno-savvy with your safety!





Theme 4: Smart Apps

4.1 Social Media

Social media is so much part of the way we interact with our friends and family. Most learners say that they feel lost if they can't access the social media platforms, where they chat and stay up to date with the latest news in their social groups. For many people, it has become an addiction!

Social media platforms will, because of the traffic and time spent on these platforms, be the perfect platform for cyber criminals, for instance:



- Cyberbullying mostly happens on social media. Remember that any information, posts or photos of you or your friends, can be used against you to spread false rumours or send you threatening and hurtful messages.
- Make sure that you know who you befriend. Criminals will use fake profiles to get to your information or lure you into dangerous online situations, like sexting and buying fake products.

Remember: Your social media settings must always be on private, and not on a public setting.

4.2 Safe Web Browsing

The **World Wide Web (WWW)** is a network of online content that is formatted and in interlinked pages, that can be accessed over the Internet. You can find anything you want to know, or need, by searching on the Internet. With all the freedom of being able to do web browsing, comes responsibility.

Let's look at some of the terms used on the web, and what it means, in order to make sure we protect ourselves while on the web.

- **Web browsing** - A web browser is a software program that allows a user to locate, access, and display web pages. Browsing or surfing the web, means that you are looking for a particular web page that you want to access.
- **Safe search** - making sure that you are not in danger of landing on a dangerous website by searching in a safe way. This means that you have to make sure to update your web browser that will help you to do safe searching.
- **Age restriction** - it means that you may be too young to access some websites, because the content is not suitable for your age.
- **Two - Factor** - It is a second layer of security on top of providing a password, that a user must provide before given access to an account or an app.
- **Unsecure website** - A website that has not been checked out to see if it is legit, that might be a threat to your cyber safety.

4.3 Gaming

Gaming apps are big business and online gaming is fast becoming a professional sport! It is also good for developing concentration and thinking skills, and a good way to make friends with other online gamers.

- Gaming sites are also being targeted by cyber criminals and online predators. Remember to make sure to check who you are gaming with, and be careful not to give too much information about who you are.
- Use a vague username that cannot be used to identify you. Sharing your personal strengths and weaknesses, might also be used against you and cause cyberbullying or make you a target for online predators.

You will enjoy online gaming much more if you are aware of the dangers and protect yourself properly. Only you can take charge of your cyber safety!





Theme 5: Useful Information



It is important to understand how to protect yourself from unwanted information or scams, as well as to protect your information from cyber criminals.

For theme 5 we have **CRYPTO** with the power to scan for sensitive information and help to lock it down before the baddies get their hands on it.

5. Useful Information - Topics:

Topic	5.1	Offensive and Inappropriate Content
Topic	5.2	Cyber Scams
Topic	5.3	Password Management

Introduction

Welcome to cyber safety theme five: Useful information. There is a huge selection of platforms in cyberspace to use, and it gets updated or replaced with better versions all the time. What was created, stored and shared yesterday, might be seen as outdated very quickly. It is important to understand how to protect yourself from unwanted information, as well as to protect your information from unwanted access. We are going to look at the value of all the information to cyber criminals, and how to protect ourselves in cyberspace with good passwords and safe searching on your devices.

Statistics/Interesting Facts

It is therefore important to know the facts about information:

DID YOU KNOW?

- Did you know that cybercrime costs the world more than R1 trillion?
- Did you know that 71% of accounts use the same passwords on multiple websites?
- 51% of 12-year-olds and 28% of 10-year-olds now have a social media profile, meaning they could be exposed to offensive and inappropriate content not in line with their age restrictions.



- Most learners don't think that the social media setting "friend of friends" could be dangerous.
- The most commonly used passwords are still password, 123456 and 12345678.
- Snapchat is ranked as the second worst app for learner's mental health.
- Nighttime use of social media and the emotional effects of social media are linked with poor sleep quality and higher levels of anxiety and depression.

Cyber Safety Tips to be discussed in this lesson

Enable safe search on your browser

Protect yourself against bad websites. Only view content that is for your age group and report sites that break the rules.

Try to keep up to date on the latest cyber scams

Cyber criminals are always busy looking for new and clever ways to scam you.

Manage your passwords correctly

Never write your password down or use the same password for all the sites you visit or use.



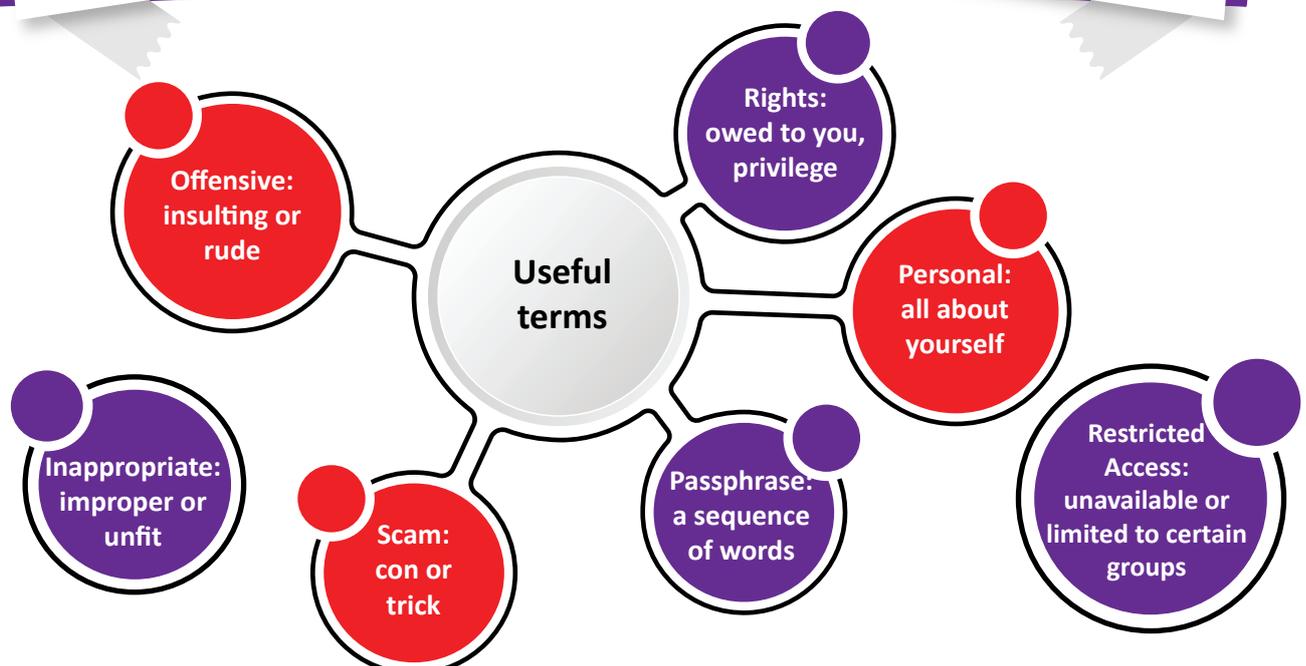
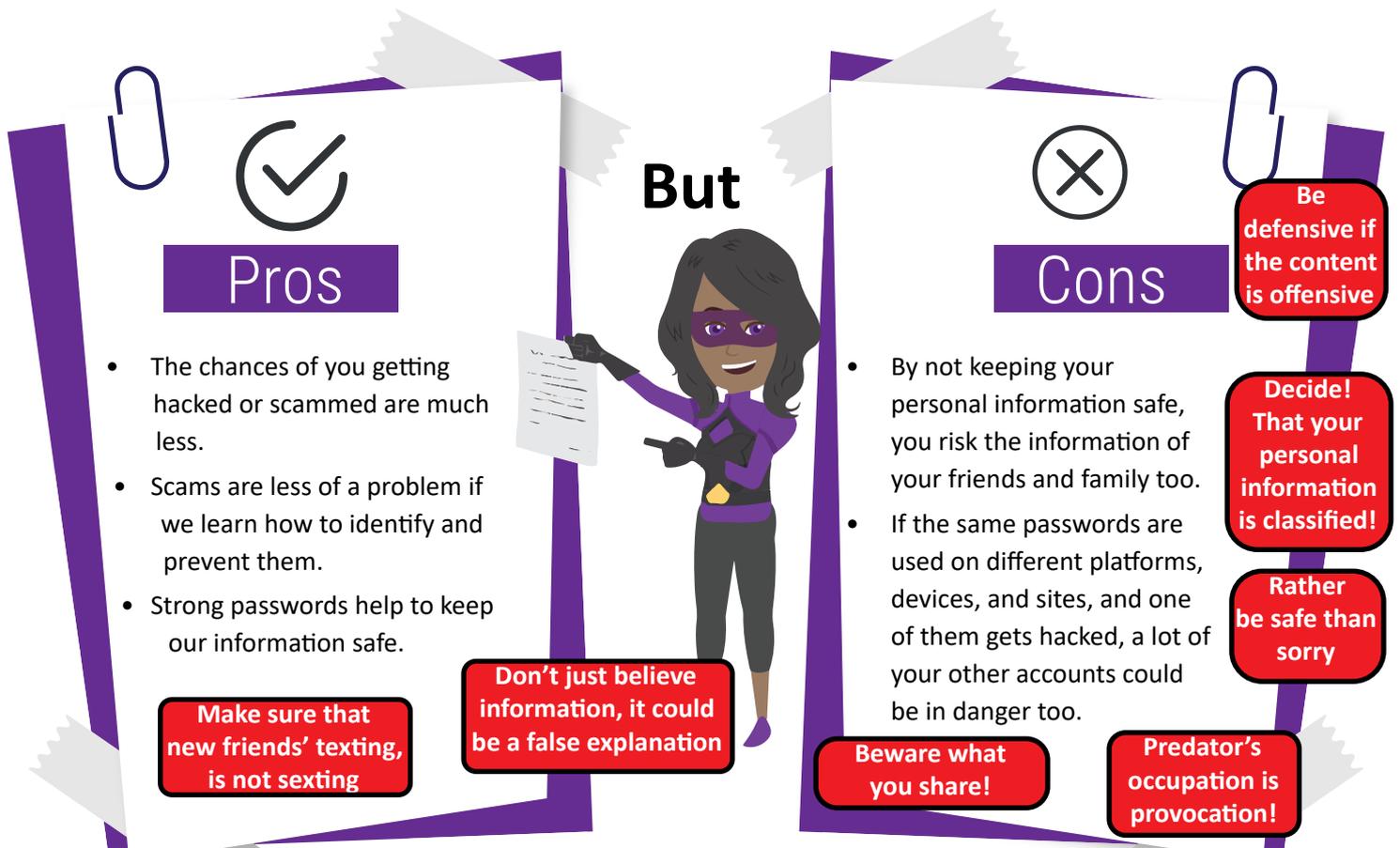


Theme 5: Useful Information

Positives of Useful Information and Vulnerabilities

It is important to understand how to protect yourself from unwanted information or scams, as well as to protect your information from cyber criminals. Social media websites are the perfect way for scammers and sexual predators, to befriend you in order to get you involved in content that you should not experience at your age, or even worse, make you a victim of scams.

Here are some of the reasons why you need to keep your personal information safe and enable safe browsing on your device:





Theme 5: Useful Information

5.1 Offensive and Inappropriate Content

It is sometimes hard to decide if the content on a specific platform, is really in your best interest and on your emotional level and age level. Always tell your parents or caregivers which social platforms you use, and websites you visit for information and new apps. They can help you to stay safe and to report offensive platforms in cyberspace.

You can change the way you interact in cyberspace, and put safety rules in place, by keeping the following in mind:

- **Watch out for fake profiles!** You really can't trust all new friend requests or emails from unknown people.
- **Sexual predators** are betting on the fact that you will not see the dangers and that you won't tell a responsible adult about inappropriate content.
- **Don't be ashamed if you are a victim.** Report cybercrime so that the criminals can be caught. This way, you will be a responsible cyber citizen that helps to put a stop to bad, harmful content and scams.
- **Share information** on which websites and platforms could be a threat to your safety with your friends. Group awareness is powerful!

5.2 Cyber Scams

Remember: Anti-malware software and a good firewall on your computer and other devices, is not a "nice-to-have", It is a "MUST HAVE"! By now, you probably understand how unsafe cyberspace can be. Scammers prey on vulnerable, innocent and ignorant cyber users, and the fact that there are so many scams and dangerous websites in cyberspace, must give you an idea of how much money and power is at stake. Just to recap:

Cyber criminals need your personal information (and your attention or "friendship"), to:

- Lure you to "free apps" and other "free goodies", just for you to find out that they want money or information from you. The saying: "Nothing in life is free" is a good motto to remember in cyberspace.
- Sell your information to marketers and fill your inboxes with loads of spam.
- Use your information, including photos and posts on social media, to stalk you and your friends.
- To bully you into being hurt, or worse, intimidate you into doing things online that is inappropriate.
- Use your information to harm you and disable your devices.

5.3 Password Management

Your main defence against cybercrime, is your password. Your password belongs to you, and it is an important responsibility to make sure that it is strong and difficult to hack. Stay in charge of your safety by following the tips and rules around passwords. For instance, not to use the same password on all your devices and on all the platforms that you use.



When someone tries to hack your password, the first thing they try is usually to see if you use your real name or gamer ID, your date of birth, or the word "password", followed by a sequence of numbers.

Your password must not be known to anyone but you, don't even give your password to your best bud!





CYBER CADETS

Guiding You Through Cyberspace



CYBER SAFETY AWARENESS PLEDGE

I recognise that...

I have the right to use electronic devices for my development.

I need to better my knowledge of the physical and digital world I live in.

I have the right to protect myself from risks and threats in cyberspace.

I have a digital footprint which needs to be protected.

However, I understand...

It is risky to share my sensitive personal information with strangers.

I have a duty to report any offensive and inappropriate content to a responsible adult.

To only use strong passwords, not write my passwords down or use the same password across multiple sites.

Therefore, I will...

Be a responsible cyber citizen and always think before I post.

Heed the guidance and rules on cyber safety of my parents and caregivers.

Show respect to others online.

Protect myself and all the people I care about by being cyber safe.



British
High Commission
Pretoria

UNISA



For further information visit:

<https://www.cybersecurityhub.gov.za/cyberawareness/>

<http://cyberaware.co.za>



CYBER SAFETY AWARENESS TIPS

CYBER CADETS

Guiding You Through Cyberspace



A Trip Into Cyberspace



Maintain a responsible digital footprint -

Realise that the content you create or share, may be stored in cyberspace forever.

Be aware of cyber risks and threats - You have the right to be safe online but also remember to behave in a decent and responsible way.

Be wary of sharing your personal information - Information may be stolen and used by criminals or sold to marketers.

Protecting People



Report cyberbullying - If you are a victim of bullying, keep evidence of the bullying. Remember that you have rights as per the 2011 Harassment Act of SA. Tell a trusted adult, don't ignore it, report it!

Be aware of both physical and cyber threats - By knowing about all the dangers and threats, you can keep yourself and your family safe.

Show respect to yourself and other people - Being online does not mean that you have the right to behave badly.

Securing Devices



Educate each other - Help one another by passing on info on new apps, sites, technologies, and threats – always share and communicate.

Keep your mobile devices safe and secure - Make sure that your devices are secured by a passcode or password. Also ensure that your sensitive personal information can be remotely deleted.

Protect against malware - Update all apps and install reputable anti-malware software on all your devices.

Smart Apps



Understand social media - There are loads of social media platforms for all tastes – good and bad! Choose wisely.

Be safe when web browsing - Only use secure and legit websites with a good reputation for online browsing. Ensure that there is a lock icon at the top of your browser.

Take precaution on all apps and gaming platforms - Use a vague username and never share personal information or your address with people you meet online.

Useful Information



Enable safe search on your browser - Protect yourself against bad websites. Only view content that is for your age group and report sites that break the rules.

Try to keep up to date on the latest cyber scams - Cyber criminals are always busy looking for new and clever ways to scam you.

Manage your passwords correctly - Never write your password down or use the same password for all the sites you visit or use.



British
High Commission
Pretoria

UNISA

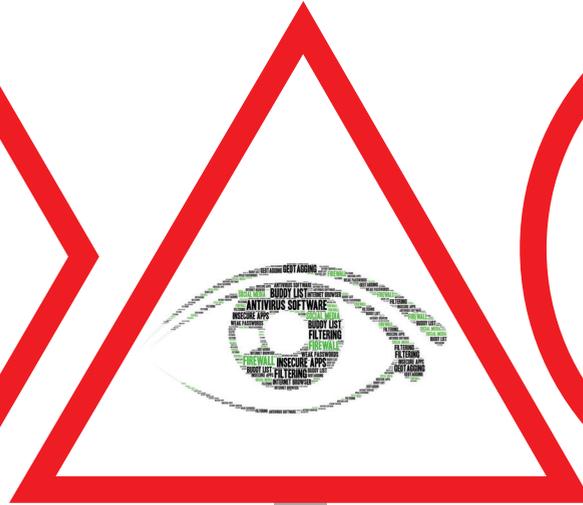
college of
science, engineering
and technology

For further information visit:

<https://www.cybersecurityhub.gov.za/cyberawareness/>
<http://cyberaware.co.za>



CAUTION: BE SAFE ONLINE



STOP

Be careful of accepting online invitations and friendships.

LOOK

Do not knowingly access or share links to inappropriate sites, upsetting or distressing content.

DECIDE

You can never be sure of the true identity of unknown DM senders. If you have any concerns or problems while online, you need to tell someone you can trust.



CYBER CADETS

Guiding You Through Cyberspace

Part of the Cyber Safety Awareness Toolkit for Learners



British High Commission Pretoria

UNISA



For further information visit:

<https://www.cybersecurityhub.gov.za/cyberawareness/>
<http://cyberaware.co.za>





British
High Commission
Pretoria

UNISA



For further information visit:

<https://www.cybersecurityhub.gov.za/cyberawareness/>
<http://cyberaware.co.za>

