CYBER CADETS

Guiding You Through Cyberspace

CYBER SAFETY AWARENESS WORKBOOK

PART OF THE CYBER SAFETY AWARENESS TOOLKIT FOR LEARNERS

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

CYBERSECURITY HUB

Table of Contents

Foreword

Cyber Safety Theme 1: A Trip into Cyberspace

Cyber Safety Theme 2: Protecting People

Cyber Safety Theme 3: Securing Devices

Cyber Safety Theme 4: Smart Apps

Cyber Safety Theme 5: Useful Information

Foreword

BRITISH HIGH COMMISSION

British
High Commission
Pretoria

Nigel Casey

British High Commissionner to South Africa

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.

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.

Foreword

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.

Foreword

UNIVERSITY OF SOUTH AFRICA

UNISA college of science, engineering and technology

Professor Elmarie Kritzinger

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 intensions.

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

Introduction

An Introduction to this Workbook

Welcome to the Teachers' Guide and School Learners' Workbook.

This workbook is aimed at school teachers and learners.

The aim and key objectives of this workbook are to educate the learners about cyber safety, by

1. **Equipping the teacher,** to utilise the cyber safety content to the best advantage and in the best possible interest of the school, community and parents (and other caregivers) in the community.
2. Providing guidelines and effective tools for your lessons, to create awareness for school learners regarding cyber safety, including:
   - **Dedicated pages** with lesson content and worksheets broken down into five cyber safety themes.
   - **Suggestions on interesting and effective ways** to conduct each lesson and an indication of additional tools for each theme. For instance, if there is specific content available for the specific theme, with the information of where it can be viewed or downloaded. **(Please see detail at the end of this page)**
   - **Ideas on how to get the learners to participate,** including suggested discussions and group work activities to encourage participation.
   - **Application and re-enforcement of learnt skills and knowledge in** the form of cartoons, word searches and questions to be answered.
3. **Providing the learners with the knowledge** they need about cyberspace and cyber safety with the aid of the Cyber Safety Awareness Toolkit.

The complete Cyber Safety Awareness Toolkit, of which the workbooks are one component, is designed around a specific, learner friendly Cyber Cadet for each theme:

- Theme 1 (A Trip into Cyberspace) we have **General Flame**. The leader of C^2 – 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.

Please remember that you will have access to the complete Cyber Safety Awareness Toolkit, designed to be a useful aid in the classroom as part of your lesson plan.

Online Platform

Workbooks

Word Searches

Videos

Posters

Cartoons

Games

For further information visit:
https://www.cybersecurityhub.gov.za/cyberawareness/
http://cyberaware.co.za

Introduction

Workbook Lessons and Themes

A Trip Into Cyberspace

THEME 1

A TRIP INTO CYBERSPACE

- Topic 1.1 Digital Footprint
- Topic 1.2 Cyber Risks and Threats
- Topic 1.3 Online Privacy

Protecting People

THEME 2

PROTECTING PEOPLE

- Topic 2.1 Cyberbullying
- Topic 2.2 Family Safety
- Topic 2.3 Communication, Respect and Ethics

Securing Devices

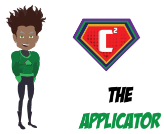
THEME 3

SECURING DEVICES

- Topic 3.1 Technology Threats
- Topic 3.2 Mobile Devices
- Topic 3.3 Malware Protection

Smart Apps

THEME 4

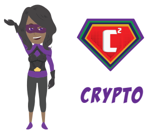


SMART APPS

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

Useful Information

THEME 5



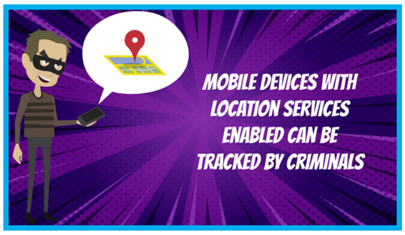
USEFUL INFORMATION

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

These topics will include content about important cyberspace terminology and advantages versus disadvantages of being a cyber citizen that is active in cyberspace.

The learners will have the opportunity to get to know the facts and apply the content of the video and the facts in the Cyber Safety Awareness Guide, by discussion, reflection and completing worksheet activities related to the specific theme.

Videos

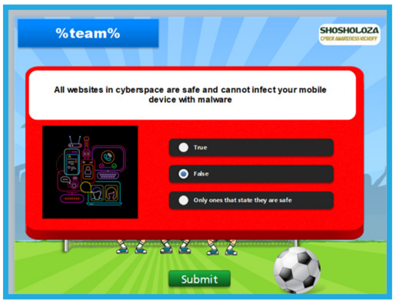


Please make sure to use the rest of the Cyber Safety Awareness Toolkit – it is a valuable aid and designed to help you as a teacher and the learners.

Posters

JOIN US ON A
CYBER SAFETY AWARENESS JOURNEY
CYBER CADETS
Guiding You Through Cyberspace
UNISA

Video Games



All websites in cyberspace are safe and cannot infect your mobile device with malware

- ○ True
- ○ False
- ○ Only ones that state they are safe

Remember, for further information visit:
https://www.cybersecurityhub.gov.za/cyberawareness/
http://cyberaware.co.za

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. FACT: Social networking drives the lives of learners… and most of it is online. Lately, we live in two worlds: physical and digital. It is important to understand what it means to be "online" and all the aspects of a digital world, or as it is called, **cyberspace**. It is so exciting to have so much information at your fingertips!

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

Let's look at some useful lingo that applies to cyberspace and cyber safety:

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, or any other device to go online.
If you use cyberspace, you are a cyber citizen. Protect yourself through cyber safety.

Cyber safety is about how to stay safe when you are online in cyberspace. There are just as many dangers to your safety and wellbeing in cyberspace, as there are in the physical world.

- **Access -** To access something, you enter it, for instance, to get onto the Internet. It can also mean to get or use something, for instance getting information.
- **Device -** A piece of electronic equipment that contains a computer, like a cell phone.
- **Internet -** A global computer network. The Internet is a network, or system, that connects millions of computers worldwide.
- **Online -** Controlled by or connected to a computer.
- **Post -** To announce or publish something.
- **Settings -** An adjustment in a software program or hardware device that adjusts it to the user's preference.

Cyberspace is full of threat agents like predators, cyberbullies, cyber criminals and scammers.
Here are some of the advantages of being cyber safe:

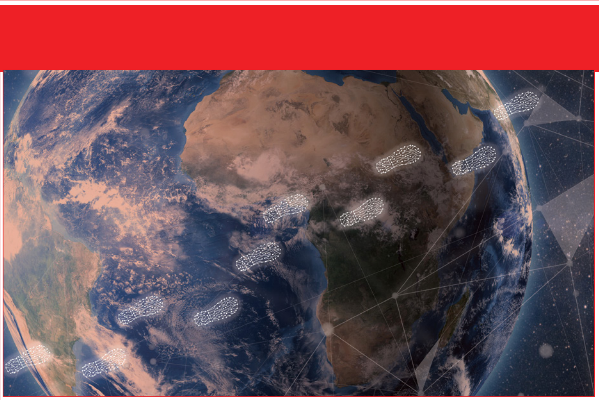
- By being aware you may **avoid clicking on "free content"** that lures you to open viruses, malware and ransomware.
- **I am safe; we are safe.** Being cyber safe will protect you from a range of threat agents - online predators, bullies, criminals and the various tools and techniques they use. Practising good online habits benefits 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.

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.



See the rest of the Cyber Safety Awareness Toolkit at:
https://www.cybersecurityhub.gov.za/cyberawareness/ - http://cyberaware.co.za

A Trip Into 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**

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.

If you are active in cyberspace, you become a cyber citizen. To be a responsible citizen, you must know how to have a good digital footprint. Here is how:

- **Think before you post or share** anything online, because it can never be deleted. What you do in cyberspace, will create a profile of who you are and what kind of person you are. If you do not show your responsible and best side, it could really influence your future, because your footprint will be used to judge your character when you apply for bursaries, jobs or future studies.
- **It is really a bad idea to share** too much of your life, where you live, contact details and information about your friends and family. Cyber criminals can't wait to get your information, to steal your identity, stalk you and harm you in any way they can. Always check your privacy settings - your cyber safety is key!

1.2 Cyber Risks and Threats

There are many risks and threats in cyberspace.

A risk means that you are seen as a potential target to crime. This doesn't mean that we must stop living or using the digital world to learn, socialise and have fun - if we are aware of the dangers, we can protect ourselves.

A threat is when there is a chance that you can be harmed in all sorts of ways. This is usually with the intention of hurting you and not by accident.

Threat agents - People that use cyberspace to hurt or steal from 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** - 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.

Computer crimes are becoming popular and are hard to stop because of the growth rate of technology.

- Never enter personal information or credit card information on unsecure websites.
- Never reply to or click on any links that you are not familiar with, and never respond to an email or advertisement saying you have won something.

1.3 Online Privacy

- **Online -** Controlled by or connected to a computer.
- **Personal privacy -** A person's private space that is not supposed to be known by others.
- **Passwords** should be a combination of upper and lower-case letters, special characters and numbers.
- Consider using a **passphrase** that is easy to remember and hard for someone else to guess, for example Gold1Lock$_3bears.
- **Never write your password** down or use the same one on multiple sites.
- Be sure to **log out of apps or websites** where important passwords are used.

Cyber criminals want your info to sell or use for cybercrime

Keep your passwords secret. (Don't even tell your best bud)

Don't get robbed of your info or attacked by malware

Decide that your personal info is classified!

"Free content" and "free websites" are usually traps

Don't open links if you don't know the sender

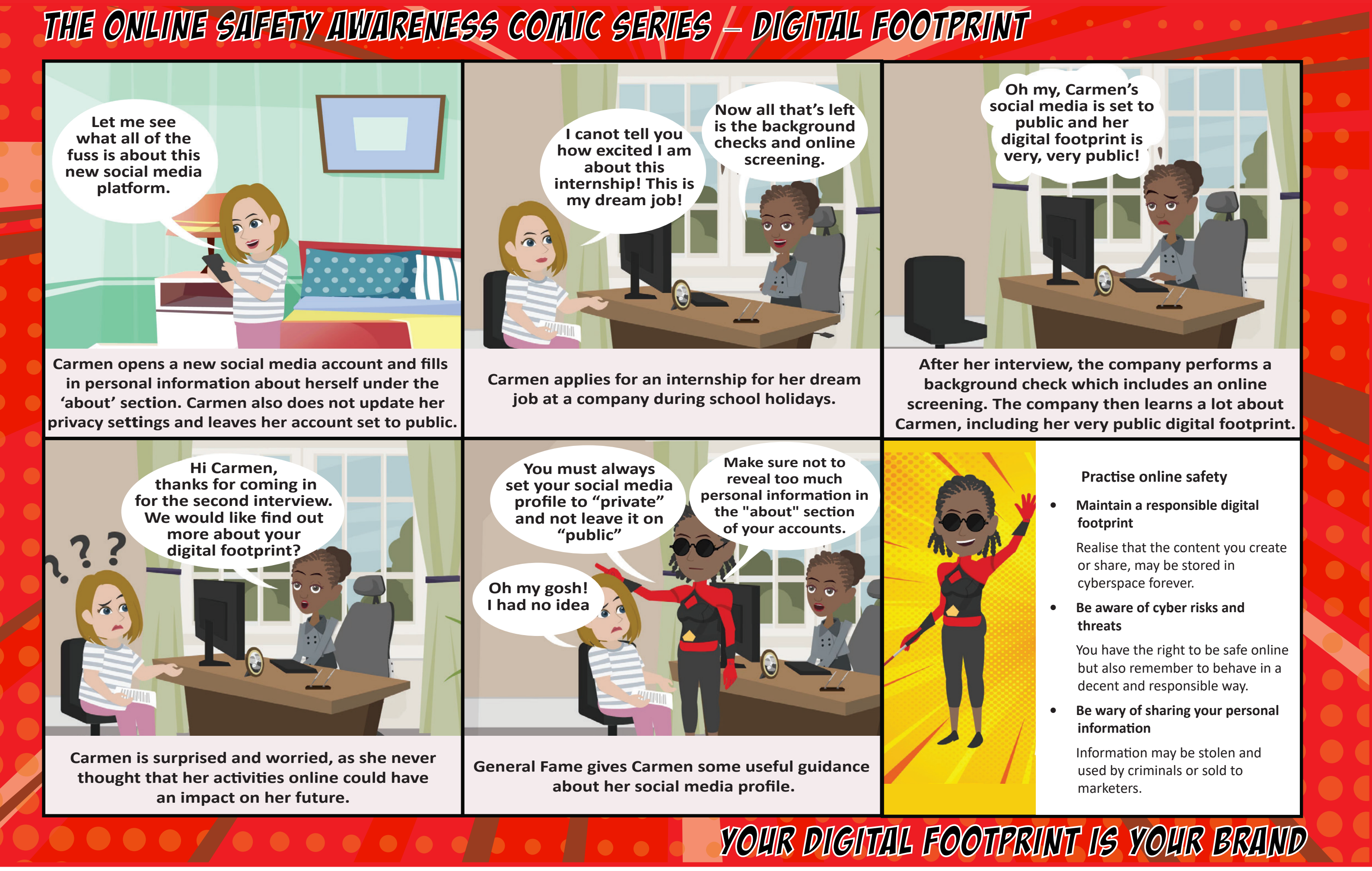
Class Activity

A TRIP INTO CYBERSPACE WORD JUMBLE

Unscramble the security words below.

N N L I O E	□□□□□□
B Y Y E R C U L B L	□□□□□□□□□□
T R T I N E N E	□□□□□□□□
R E W M L A A	□□□□□□□
T S T E A R H	□□□□□□□
K R B E R Y I S C S	□□□□□□□□□□
C R V P A Y I	□□□□□□□
F O N I T A L D I O T P R I G T	□□□□□□□□□□□□□□□□
N I I H H P S G	□□□□□□□□
P K A U C B	□□□□□□
F W I I	□□□□

Cartoon


THE ONLINE SAFETY AWARENESS COMIC SERIES – DIGITAL FOOTPRINT
Let me see what all of the fuss is about this new social media platform.
Carmen opens a new social media account and fills in personal information about herself under the ‘about’ section. Carmen also does not update her privacy settings and leaves her account set to public.
I canot tell you how excited I am about this internship! This is my dream job!
Now all that’s left is the background checks and online screening.
Carmen applies for an internship for her dream job at a company during school holidays.
Oh my, Carmen’s social media is set to public and her digital footprint is very, very public!
After her interview, the company performs a background check which includes an online screening. The company then learns a lot about Carmen, including her very public digital footprint.
Hi Carmen, thanks for coming in for the second interview. We would like find out more about your digital footprint?
? ? ?
Carmen is surprised and worried, as she never thought that her activities online could have an impact on her future.
You must always set your social media profile to “private” and not leave it on “public”
Make sure not to reveal too much personal information in the "about" section of your accounts.
Oh my gosh! I had no idea
General Fame gives Carmen some useful guidance about her social media profile.
YOUR DIGITAL FOOTPRINT IS YOUR BRAND

Practise online safety

- **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.

Cartoon Questions

1. What is the first thing Carmen did wrong?

....

2. What is the second thing Carmen did wrong?

....

3. Why is it important to have a responsible digital footprint?

....

4. What do you think would have happened if General Flame did not appear?

....

5. What did you learn from this cartoon?

....

6. What message would you give Carmen not to make the same mistake in the future?

....

Discussion: Divide into groups and discuss the advantages of having a responsible digital footprint. Discuss what can go wrong and how you can compromise your digital footprint. Use the following terminology or terms:

cyberspace
threat agents
respect
spread
future
personal information
online predators
social media
content
privacy settings
mistake
digital devices
cyber criminals
password protection
risks and threats
delete
safety awareness

Reflection: Write a few sentences (or draw a picture) about your online experiences, (good or bad), with social media sites or your digital footprint.

End of Theme 1

Protecting People

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. Theme 2 will help you to understand that your footprint in cyberspace, is not only about your own safety, but affects all the people around you that you care about. We will look at how you should behave when online by following the guidelines 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

Vulnerabilities of People and Threat Agents

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.

- **Threat agents** are people or groups of criminals, that use cyberspace to hurt or steal from you. (Also see theme 1 for examples and definitions of threat agents).
- **Communication** is a two-way "line" between two or more people, to share news, ideas, information and feelings. Communication can be talking to each other physically, writing messages, chatting on the phone and of course, using all the platforms in cyberspace to have contact with each other.
- **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.
- **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.**

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.

See the rest of the Cyber Safety Awareness Toolkit at:
https://www.cybersecurityhub.gov.za/cyberawareness/ - http://cyberaware.co.za

Theme 2: Protecting People

2.1 Cyberbullying

FACT: Cyberbullying is one of the biggest causes of depression and suicide amongst learners.

Cyberbullying 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.

Don't be scared to speak up if you are being bullied! By not speaking up and communicating with your parents or caregivers about being bullied, you run the risk of being alone, scared and an easy target for ongoing cyberbullying.

If you do not report cyberbullying, there is a higher chance of it happening continuously, with no end in sight.	Telling your caregiver or parent means they can open up an investigation to make sure that the cyberbully gets punished.
Your caregiver or parent can get in touch with the correct authorities and channels needed to report the cyberbullies.	It is your duty to speak up to not only stop the crime, but to spare other people from becoming victims too!

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!

2.2 Family Safety

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

THINK BEFORE YOU POST!

- **Think before you post**, you can never permanently erase something that you have posted on social media.
- **Check all privacy settings** and use strong passwords.
- **Disable location settings** on your cell phone, camera and social media sites.
- **Be careful of friend requests from strangers**. Fake profiles are often created by cyber criminals and sexual predators to get to you and your information.
- **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. Like 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

- **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.

A good cyber citizen will always communicate and behave respectfully and ethically. Here are a few ways how:

A GOOD CYBER CITIZEN

Will have a responsible digital footprint	Will protect personal information	Shows respect for other cyber citizens	Will follow cyber safety rules
Won't support fake news and will not post false information	Will be ethical in the cyber community (virtual community)		Will report cybercrime and stand up to cyberbullies

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

You can be seen as a cyberbully if you behave badly towards others in cyberspace.

Class Activity

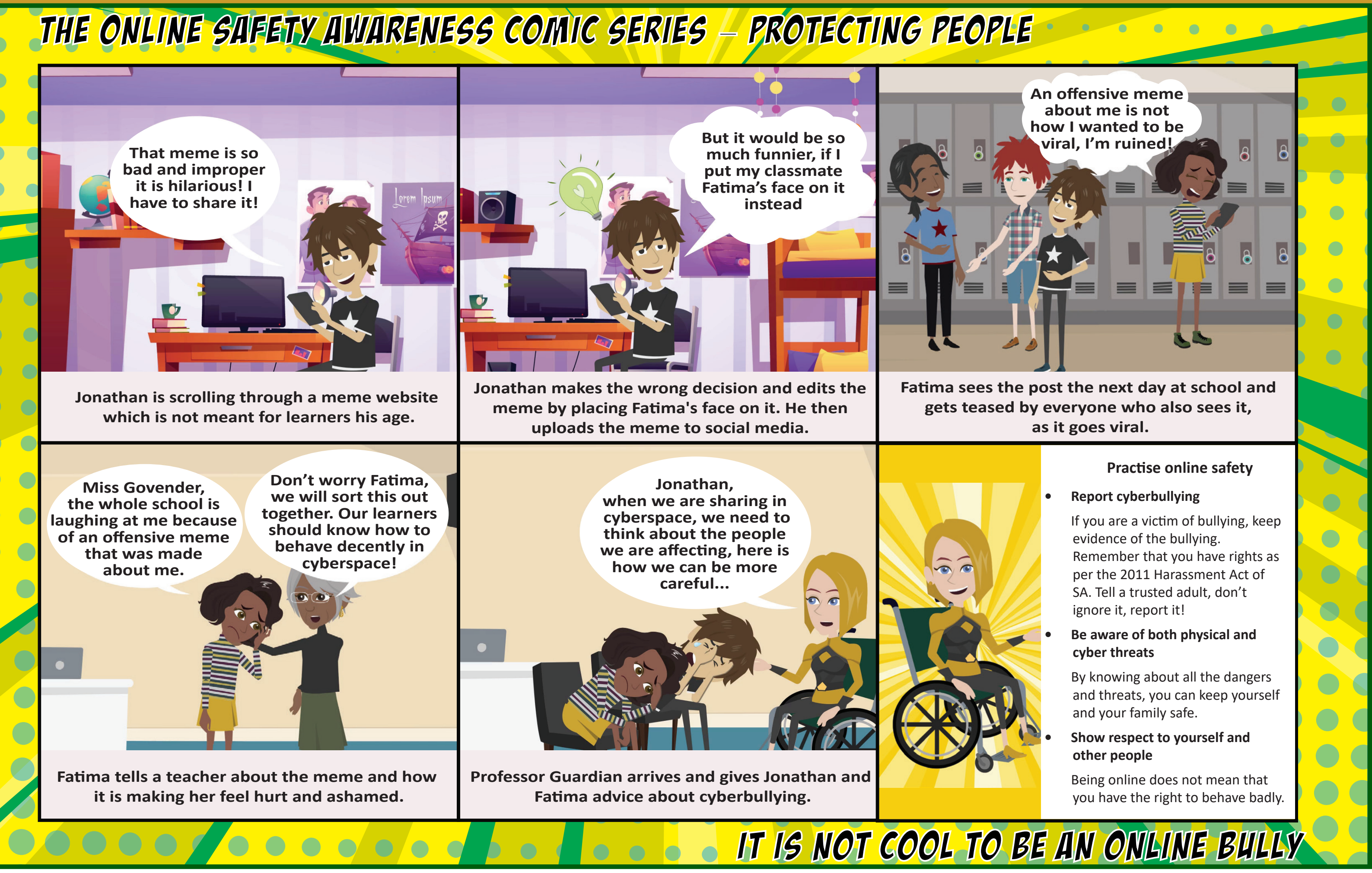
PROTECTING PEOPLE MIX-AND-MATCH

Draw a line to match the words with their definitions!

1	Cyberbullying
2	Family Safety and Communication
3	Mobile Security
4	Malware
5	PII
6	Phishing
7	Social Networking
8	Mobile Application
9	Respect and Ethics

a	A set of values or moral principles that shows how you conduct yourself in cyberspace, and how you show consideration for other people.
b	Personal information, such as your full name, school and home address, and birthday.
c	A social networking service is an online platform which people use to build social networks or social relationship with other people who share similar personal or career interests, activities, backgrounds or real-life connections.
d	Referred to as a mobile app or simply an app, is a computer program or software application designed to run on a mobile device such as a cell phone, tablet, or watch.
e	Malicious software.
f	The most common type of social engineering attack, used in 90% of data breaches.
g	Be aware of what you see and hear on the Internet, who you meet, and what you share about yourself. Talk to your parents, use tools to protect your family.
h	The protection of smartphones, tablets, laptops and other portable computing devices, and the networks they connect to, from threats and vulnerabilities associated with wireless computing.
i	Causing harm to a person through the form of electronic text via email, websites, social networking sites or blogs. It is usually done by sending hurtful or threatening messages.

Cartoon


THE ONLINE SAFETY AWARENESS COMIC SERIES – PROTECTING PEOPLE
That meme is so bad and improper it is hilarious! I have to share it!
Lorem Ipsum
Jonathan is scrolling through a meme website which is not meant for learners his age.
But it would be so much funnier, if I put my classmate Fatima's face on it instead
Jonathan makes the wrong decision and edits the meme by placing Fatima's face on it. He then uploads the meme to social media.
An offensive meme about me is not how I wanted to be viral, I'm ruined!
Fatima sees the post the next day at school and gets teased by everyone who also sees it, as it goes viral.
Miss Govender, the whole school is laughing at me because of an offensive meme that was made about me.
Don't worry Fatima, we will sort this out together. Our learners should know how to behave decently in cyberspace!
Fatima tells a teacher about the meme and how it is making her feel hurt and ashamed.
Jonathan, when we are sharing in cyberspace, we need to think about the people we are affecting, here is how we can be more careful...
Professor Guardian arrives and gives Jonathan and Fatima advice about cyberbullying.
IT IS NOT COOL TO BE AN ONLINE BULLY

Practise online safety

- **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.

Cartoon Questions

1. What is the first thing Jonathan did wrong?

....

2. Did Jonathan cyberbully Fatima? If so, how?

....

3. What did Fatima do that was correct?

....

4. What do you think would have happened if Professor Guardian did not appear?

....

5. What did you learn from this cartoon?

....

REFLECTIONS. In groups, discuss the effects of cyberbullying on learners.

- **Present it to the class and include ways to stop bullying at your school.**
- **Use the space below to make a flyer or poster promoting cyber safety awareness!**

End of Theme 2

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 instant. **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

Positives and Vulnerabilities of Devices

Devices are the physical tools that enable cyber criminals to commit online crimes.

Threat agents - people or a group of people that use cyberspace to hurt or steal from you, scam you, stalk you or bully you. For example: Cyber criminals want to plant harmful software, like a virus, malware or ransomware, on your device to damage it or blackmail you.

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

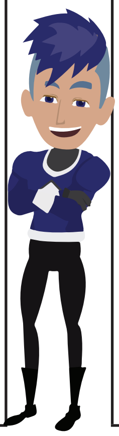
Beware of all the scams out there and what you share!

Enable safe searching

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.

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

Be careful when you use public Wi-Fi

Disable location settings!

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.

See the rest of the Cyber Safety Awareness Toolkit at:
https://www.cybersecurityhub.gov.za/cyberawareness/ - http://cyberaware.co.za

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!

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!

Due to the high use and growth rate of technology, cyber scams and cyber fraud have disrupted bank accounts, sent viruses, and stolen personal information.

Being aware of all the technology threats, will make us much safer in cyberspace:

- By being cyber aware, you may avoid clicking on “free content” that is really just a way of downloading viruses, malware and ransomware.
- You will be sure to protect yourself, your family and your friends too by keeping your information safe.
- Being cyber safe will protect you from getting viruses on devices – An anti-virus is still a must.

Remember:

- Never enter personal information or credit card information on unsecure websites.
- Never reply to or click on any links that you have not used before, and be careful of friend requests from strangers.
- Do not respond to an email or advertisement saying you have won something.
- Check all privacy settings and make sure that you have good anti-malware software installed on your devices.

3.2 Mobile Devices

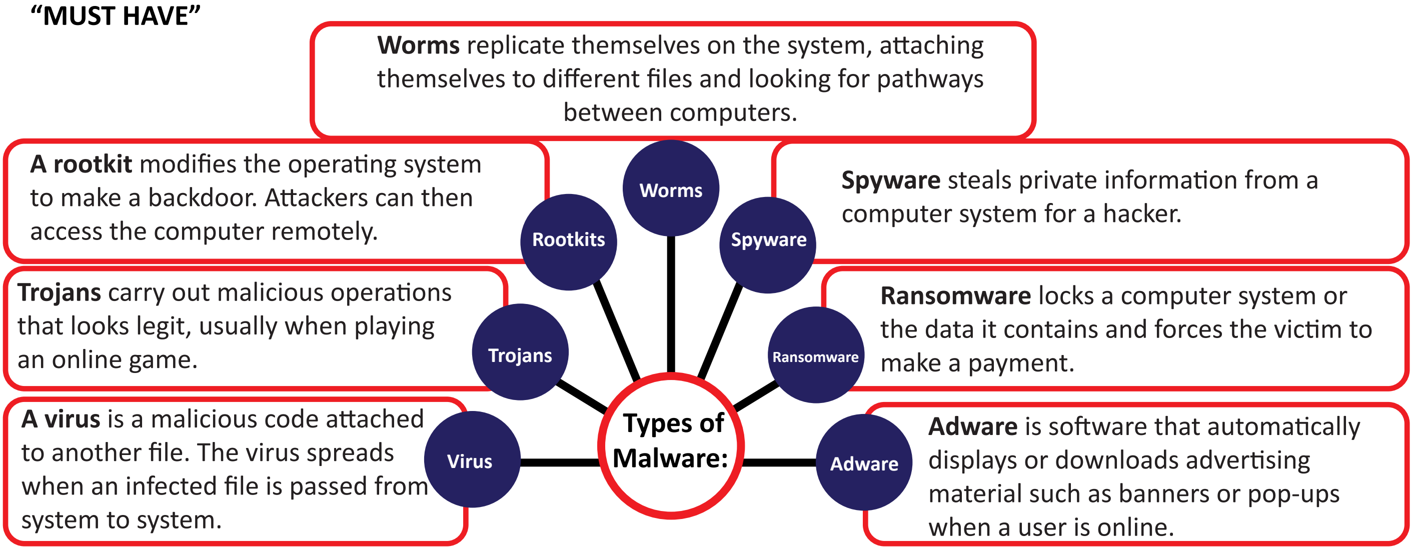
Device - A piece of electronic equipment that contains a computer, like a cell phone.

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

- 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.

3.3 Malware Protection

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”**



Worms replicate themselves on the system, attaching themselves to different files and looking for pathways between computers.

A rootkit modifies the operating system to make a backdoor. Attackers can then access the computer remotely.

Spyware steals private information from a computer system for a hacker.

Trojans carry out malicious operations that looks legit, usually when playing an online game.

Ransomware locks a computer system or the data it contains and forces the victim to make a payment.

A virus is a malicious code attached to another file. The virus spreads when an infected file is passed from system to system.

Adware is software that automatically displays or downloads advertising material such as banners or pop-ups when a user is online.

Theme 3: Securing Devices

Class Activity

SECURING DEVICES WORD JUMBLE

Unscramble the security words below.

DWOPSASR □□□□□□□□

TEOYNGLOCH □□□□□□□□□□

LNEKSCRECO □□□□□□□□□□

HTEFT □□□□□

ACHEKR □□□□□□

TUYSCIER □□□□□□□□

TRHETATGENA □□□□□□□□□□□

IOLSCAAEIDM □□□□□□□□□□□

CSIMINALR □□□□□□□□□

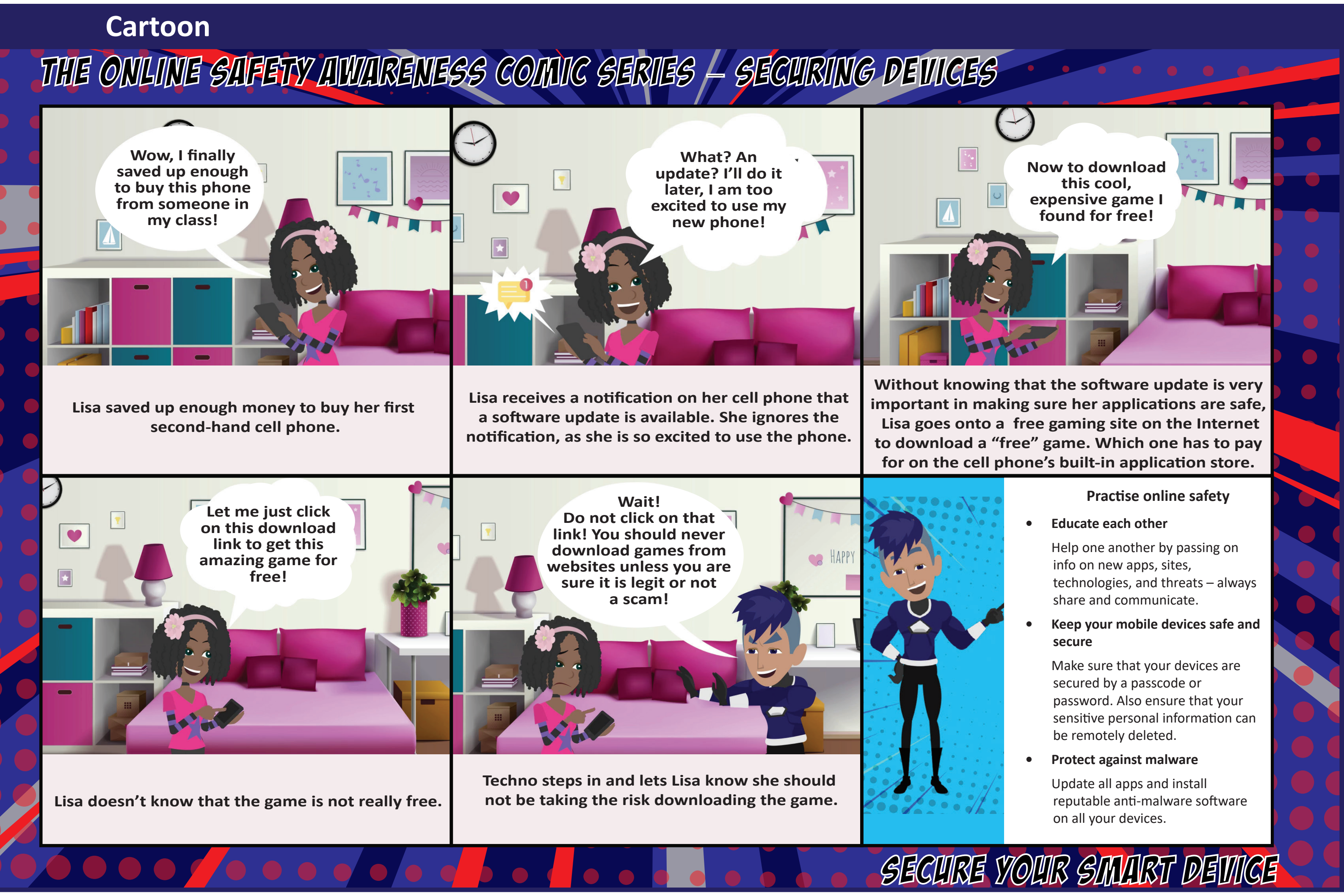
EOLIBM □□□□□□

CUREUNSE □□□□□□□□

A few visual clues to help you!”

MOBILE DEVICES WITH LOCATION SERVICES ENABLED CAN BE TRACKED BY CRIMINALS

Cartoon


THE ONLINE SAFETY AWARENESS COMIC SERIES – SECURING DEVICES
Wow, I finally saved up enough to buy this phone from someone in my class!
What? An update? I'll do it later, I am too excited to use my new phone!
Now to download this cool, expensive game I found for free!
Let me just click on this download link to get this amazing game for free!
Wait! Do not click on that link! You should never download games from websites unless you are sure it is legit or not a scam!
HAPPY
SECURE YOUR SMART DEVICE

Lisa saved up enough money to buy her first second-hand cell phone.

Lisa receives a notification on her cell phone that a software update is available. She ignores the notification, as she is so excited to use the phone.

Without knowing that the software update is very important in making sure her applications are safe, Lisa goes onto a free gaming site on the Internet to download a “free” game. Which one has to pay for on the cell phone's built-in application store.

Lisa doesn't know that the game is not really free.

Techno steps in and lets Lisa know she should not be taking the risk downloading the game.

Practise online safety

- **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.

Securing Devices

Theme 3: Securing Devices

Cartoon Questions

1. What is the first thing Lisa did wrong?

....

2. What is the second thing Lisa did wrong?

....

3. Why is it important to ensure that your mobile devices are password protected and encrypted?

....

4. What do you think would have happened if Techno did not appear?

....

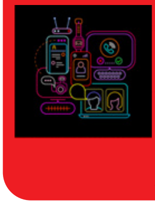
5. What did you learn from this cartoon?

....

Are you ready for a few penalty kicks?

Choose the correct answer to each question

All websites in cyberspace are safe and cannot infect your mobile device with malware



○ True

○ False

○ Only ones that state that they are safe.

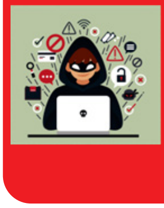
Why is it important to make sure the website you are browsing has a lock icon at the top of the screen?

○ To lock out viruses and malware.

○ To make sure your device is locked down.

○ To make sure that the website is secure.

How can we make sure that we protect our devices and keep them safe from criminals?



○ Check with your parents before downloading or installing software.

○ Nothing, smart devices should be smart enough to protect themselves.

○ Trust cyberspace and just download and install any software onto your device.

A virus is a type of computer programme that will invade, replicate itself and insert its own code to damage and infect your devices. How can you protect your devices from becoming infected whilst in cyberspace?

○ Never turn on your devices, let them gather dust.

○ Ensure that your devices' anti-virus and firewall are always kept active and up to date.

○ Trust that the device will just protect itself.

Class Discussions

NOMOPHOBIA is the fear of being away from your mobile phone, or not being able to use it, because of the lack of airtime or cell phone signal. FOMO is the Fear of Missing Out.

As a group, look at the definition of Nomophobia and FOMO. Discuss and write your thoughts down in the space provided.

- **When using your cell phone is a positive part of your life.**
- **At what point using your cell phone becomes Nomophobia.**
- **The effect on a person's life if they suffer from Nomophobia.**

End of Theme 3

Smart Apps

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 be tough on criminals and bullies that prey on the innocent.

Introduction

Welcome to cyber safety theme four: Smart Apps. Most young people know their way around cyberspace and have great skills when using technology. The whole world benefits from this instant access to information and people. Most parents also agree that it is a great way for their children to learn, socialise, and discover all the amazing things about the world we live in. All of the opportunities that you have in cyberspace today come with loads of threats and risks that we need to control and avoid while using apps on our devices.

4.	Smart Apps - Topics:	Topic	4.1	Social Media
		Topic	4.2	Safe Web Browsing
		Topic	4.3	Gaming

Smart apps are a useful part of our lives, and a few of the positives are:

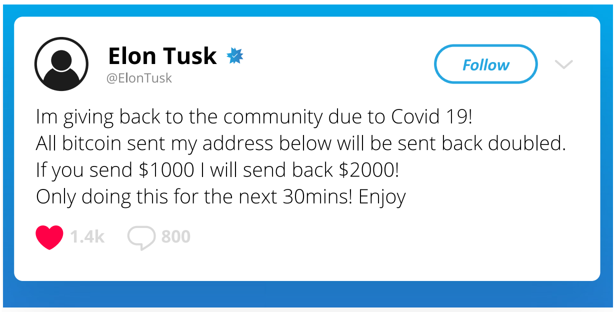
- It is so much easier to do research for school projects by browsing on the web. The web also helps you to be creative when preparing for orals and presentations.
- Parents and caregivers are less worried when you are with your friends or going off to social events, because you can reach out and make contact if you are in trouble or lost.
  However, it is important to think about aspects of social media, besides being a target of cybercrime that could be harmful to your emotional and physical state, such as:

- Spending long hours into the night on apps that will affect your sleeping habits and rest.
- Not getting enough physical exercise and fresh air- healthy body, healthy mind!
- Becoming isolated from your peers because you are not part of physical social gatherings.
- Becoming addicted to gaming and social media, so that you lose interest in real life and being part of your family and the world out there.
- Emotional problems like depression and anxiety over your image and popularity on social media.

Social media is the perfect platform for cyber criminals to attack if you give them the chance. The threat is very real. Just look at the following example of an attack that affected a lot of famous people. ⬇

We are going to look at ways to protect yourself and your devices, while you are using apps and websites. Your cyber safety is in your hands - it is your responsibility to use all the technological aids and important tips to protect yourself in cyberspace!

Don't become 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. Think before you share links with your friends that could be malware!



Elon Tusk
@ElonTusk

Follow

Im giving back to the community due to Covid 19!
All bitcoin sent my address below will be sent back doubled.
If you send $1000 I will send back $2000!
Only doing this for the next 30mins! Enjoy

♥ 1.4k 💬 800

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.

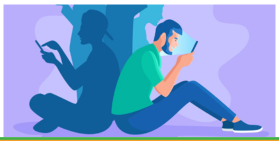
See the rest of the Cyber Safety Awareness Toolkit at:
https://www.cybersecurityhub.gov.za/cyberawareness/ - http://cyberaware.co.za

Smart Apps

Theme 4: Smart Apps

4.1 Social Media

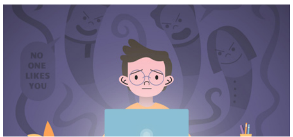
Let's look at the good and bad of social media, and how to avoid all the bad!



Social media addiction can happen by being overly concerned about social media, driven by an uncontrollable urge to log on to or use social media, and devoting so much time and effort to it that it harms other areas of your life.

If we don't make sure that our social media settings are on private, not public, criminals and predators can get access to our location. Social media and smart apps give us instant remote access to our parents, caregivers, family and friends. If your social media settings are not on private, but public, criminals and predators can get access to your location, money and Info to steal or stalk you.

We can make new friends on social media. However, think before you befriend someone. Criminals use fake profiles to attack you and your personal info in all sorts of ways. Don't become a victim to sexting or scams of fake products.



Cyberbullying happens on social media. Any posts, photos and info about you or friends, can be used to damage your reputation with false rumours and threatening or hurtful messages.

- Always ensure that sites you are visiting are HTTPS, e.g. https://www.absa.co.za which require you to supply your username and password, especially when banking or buying online. Do not access personal banking sites by using untrusted Wi-Fi networks, such as free Wi-Fi at restaurants or any other public places.
- Maintain your privacy settings!
- Disable location settings!
- Think before you post!
- Beware what you share - once said, the web is fed!

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 they mean, to make sure we protect ourselves 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 is a great way to relax and make new online friends!

Did you know? Gaming is a recognised online sport, and that international gamers make millions in prize money, by being new game "testers" and in sponsorship?

Besides being fun, gaming also helps with the development of your mind and body, if you don't overdo it.

- Gaming develops your cognitive skills, meaning your thinking and learning skills.
- It develops your fine motor control skills, like hand-eye coordination.
- It improves concentration levels and problem-solving skills.
- It sharpens your reflexes and your vision.

- 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.
- Watch out for **hidden fees** that look like freebies. Most games on the web are commercial products and requires a monthly or once off fee.
- Report suspicious gaming sites and people on the game that acts like **sexual predators**.

Smart Apps

Theme 4: Smart Apps

Class Activity

SMART APPS

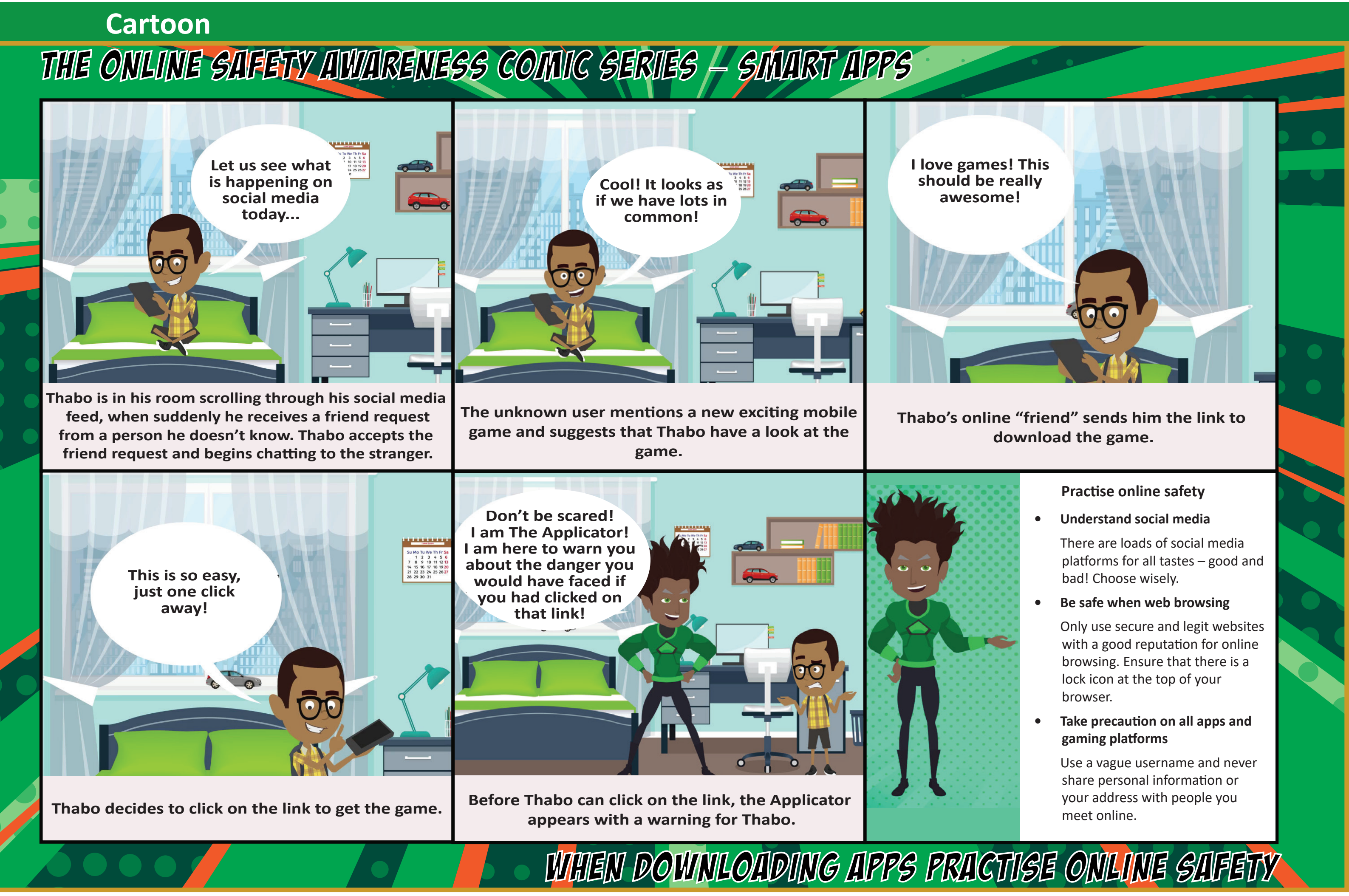
Match the clues with the words, then find it in the word search

1	Downloaded to a mobile device
2	Protection while you browse
3	Surfing websites
4	Playing online
5	Rated according to age
6	Apps
7	Sometimes referred to as two-step verification
8	Setting that shows where you are
9	Opposite of public settings
10	A dangerous site

a	Applications
b	Social Media
c	Web Browsing
d	Gaming
e	Safe Search
f	Unsecure Site
g	Age Restriction
h	Two-Factor
i	Privacy Settings
j	Location Settings

A	P	P	L	I	C	A	T	I	O	N	S	O	U	A
W	I	R	M	T	W	O	F	A	C	T	O	R	G	G
P	W	I	T	L	B	P	H	A	S	S	C	T	E	E
O	G	V	I	O	R	X	O	S	L	S	I	R	X	R
Q	A	A	H	C	K	Y	E	S	E	F	A	S	W	E
R	F	C	D	A	S	S	S	J	D	S	L	U	U	S
E	U	Y	U	T	G	A	O	S	E	B	M	K	I	T
F	N	S	E	I	X	S	F	U	M	S	E	E	H	R
T	S	E	T	O	P	E	S	E	S	J	D	F	F	I
P	E	T	K	N	C	N	B	S	S	N	I	Y	K	C
E	C	T	Y	S	N	S	A	I	Q	E	A	Z	U	T
I	U	I	Z	E	O	D	J	P	D	U	A	M	O	I
S	R	N	M	T	L	C	A	Y	O	G	Z	R	S	O
M	E	G	T	T	Y	B	G	X	R	A	F	I	C	N
I	S	S	I	I	H	M	N	I	U	M	G	Y	U	H
W	I	A	F	N	A	E	O	P	F	I	L	P	N	L
T	T	R	L	G	O	C	Q	D	R	N	I	W	M	A
W	E	B	B	R	O	W	S	I	N	G	P	V	U	D

Cartoon


THE ONLINE SAFETY AWARENESS COMIC SERIES – SMART APPS
Let us see what is happening on social media today...
Cool! It looks as if we have lots in common!
I love games! This should be really awesome!
This is so easy, just one click away!
Don't be scared! I am The Applicator! I am here to warn you about the danger you would have faced if you had clicked on that link!
WHEN DOWNLOADING APPS PRACTISE ONLINE SAFETY

Thabo is in his room scrolling through his social media feed, when suddenly he receives a friend request from a person he doesn't know. Thabo accepts the friend request and begins chatting to the stranger.

The unknown user mentions a new exciting mobile game and suggests that Thabo have a look at the game.

Thabo's online "friend" sends him the link to download the game.

Thabo decides to click on the link to get the game.

Before Thabo can click on the link, the Applicator appears with a warning for Thabo.

Practise online safety

- **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.

Cartoon Questions

1. What is the first thing Thabo did wrong?

....

2. What is the second thing Thabo did wrong?

....

3. How can you ensure that a website you are visiting is secure?

....

4. What do you think would have happened if The Applicator did not appear?

....

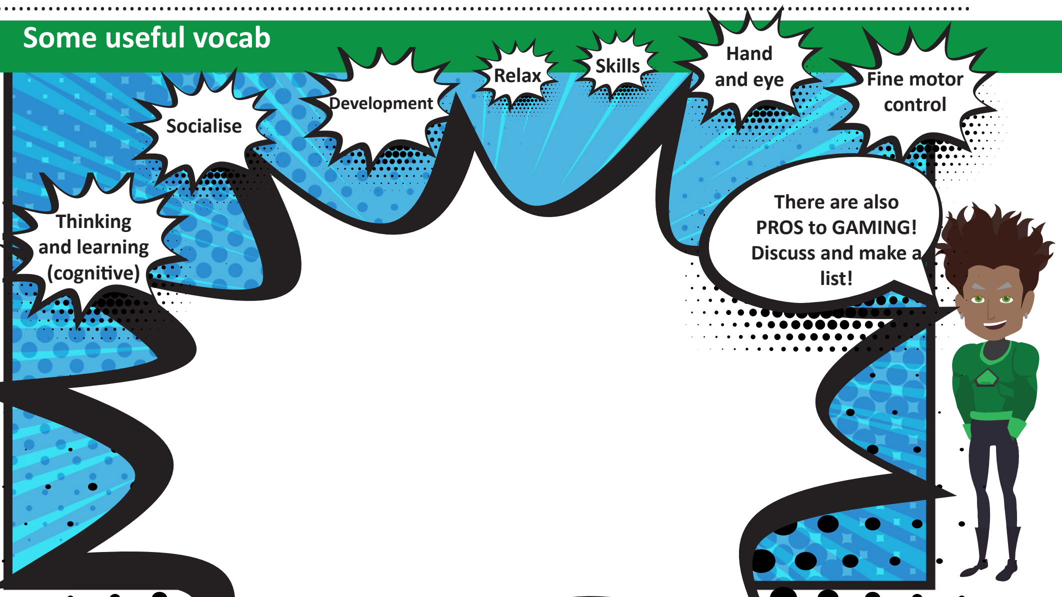
5. What did you learn from this cartoon?

....

Class Discussions

There are CONS to GAMING. The Applicator WARNS:
Vulnerabilities of gaming include cyberbullying, online predators and hidden fees

Some useful vocab


Socialise
Development
Relax
Skills
Hand and eye
Fine motor control
Thinking and learning (cognitive)
There are also PROS to GAMING! Discuss and make a list!

The Applicator needs you to create your own slogans to promote good social media behaviour

End of Theme 4

Useful Information

Theme 5: Useful Information

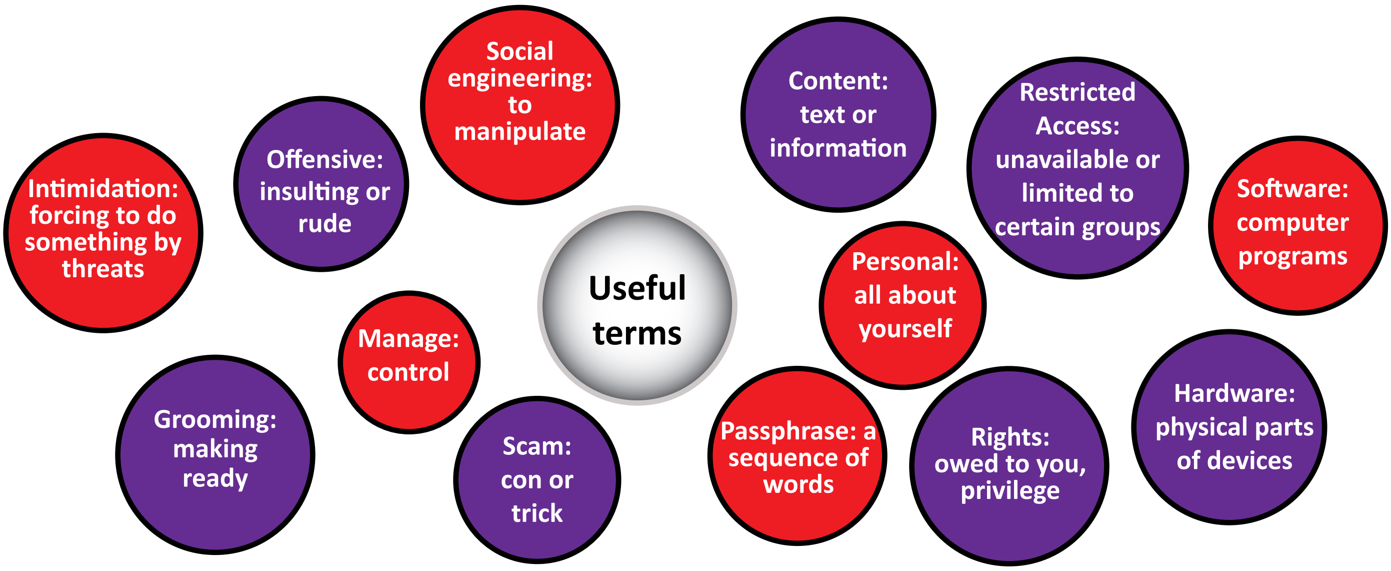
It is important to understand how to protect yourself from unwanted information or scams, as well as to protect your information from cyber criminals.

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

Introduction

Welcome to cyber safety theme five: Useful Information. Cyberspace has created the chance to change the way we live our lives, by providing state of the art devices, software and social media platforms. Businesses, governments and world news depend on cyberspace to function and to store information. It creates many opportunities for cyber criminals to hack for financial gain, political gains and espionage between businesses and countries. Not to mention crime against you as a person through bullying, and being targeted by sexual predators, as well as infecting devices with viruses!

5.	Useful Information - Topics:	Topic	5.1	Offensive and Inappropriate Content
		Topic	5.2	Cyber Scams
		Topic	5.3	Password Management



Useful terms

Social engineering: to manipulate

Content: text or information

Restricted Access: unavailable or limited to certain groups

Offensive: insulting or rude

Intimidation: forcing to do something by threats

Software: computer programs

Personal: all about yourself

Manage: control

Grooming: making ready

Scam: con or trick

Passphrase: a sequence of words

Rights: owed to you, privilege

Hardware: physical parts of devices

There are many reasons why it is important to protect your personal and private information. Here are a few:

- The chances of you getting hacked or scammed are much less.
- Scams are less of a problem if we learn how to identify and prevent them.
- Strong passwords help to keep our information safe.

We are going to give you the tools to protect yourself against scammers and predators, so that you will put proper protection in place.
Watch out for the following:

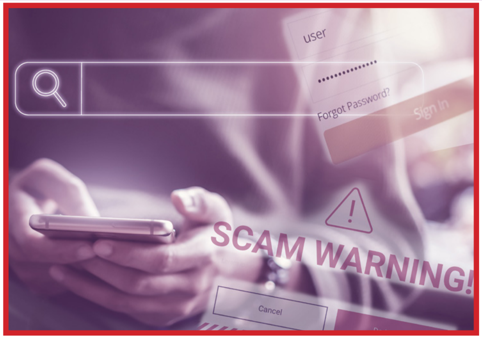
- Public settings that put your personal information at risk, and the information of your friends and family too.
- If the same passwords are used on different platforms, devices, and sites, and one of them gets hacked, a lot or all of your other accounts could be in danger too.
- The types of social engineering used by scammers, hackers and predators.

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.



Useful Information

Theme 5: Useful Information

5.1 Offensive and Inappropriate Content

You can't always tell the difference between a fake profile or a real one, or which websites are legit. Predators are also so clever that you do not always catch on immediately to their true intentions before it is too late.
Luckily, there are many ways to stay safe if you follow some good common sense and safety rules.

A predator's occupation Is sexual provocation

Make sure that a new friend's texting is not sexting

Be defensive if the content is offensive

Report inappropriate content. 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.

Always tell your parents or caregivers which social platforms you use, and websites you visit for information and new apps. They can help you stay safe and report offensive platforms in cyberspace.

Turn on safe-surfing options and keep up to date with the latest Internet trends to maximise your safety.

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

Due to the high use of the Internet, cyber scams and cyber fraud has disrupted bank accounts, sent viruses, and stolen personal information. 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. 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.

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 are inappropriate.
- Use your information to harm you and disable your devices.

- **Never enter personal information** or credit card information on unsecure websites.
- **Never reply to or click on any links** that you have not used before, and never respond to an email or advertisement saying you have won something.
- **Always keep up to date with the latest cyber threats**. Share information with each other and report any harmful sites and activities.
- Avoid falling victim to cybercrime, by **understanding the various cyber criminal tactics**, used by attackers to gain confidential information.
- **Use strong passwords** and user accounts and remember to log out of sensitive accounts.
- **Only shop on trusted sites** which have a good reputation and a secure connection. Never make use of public Wi-Fi when shopping online, as cyber criminals are known to intercept connections in order to obtain information.
- **Always ensure that sites you are visiting** are HTTPS e.g. https://www.absa.co.za which require you to supply your username and password, especially when banking or buying online.

5.3 Password Management

Did you know? 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 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 regarding passwords:

- Passwords should be a combination of upper- and lower-case letters, special characters and numbers.
- Consider using a passphrase that is easy to remember and hard for someone else to guess, for example Gold1Lock$_3bears.
- Never write your password down. Do not use the same password on all your devices and on all the platforms that you use.
- Be sure to log out of apps or websites where important passwords are used.

Decide that your personal info is classified!

Beware what you share!

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

Class Activity

USEFUL INFORMATION

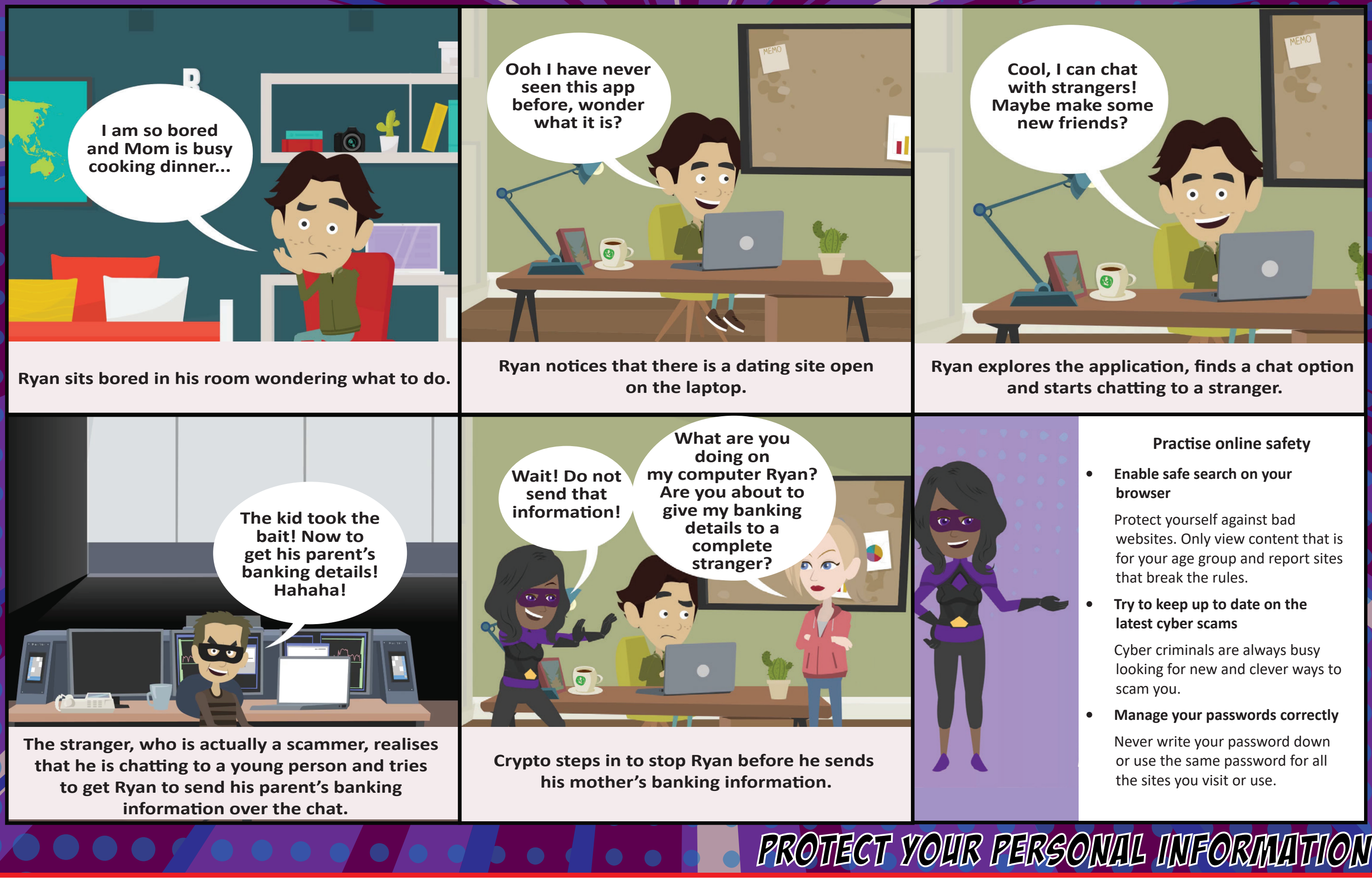
Give a meaning for the following words. Then find it in the word search

Information	-	
Offensive	-	
Inappropriate	-	
Scam	-	
Strong Password	-	
Passphrase	-	
Personal	-	
Restricted Access	-	
Rights	-	
Cybersecurity	-	

I	N	A	P	P	R	O	P	R	I	A	T	E	A	I	R
N	S	T	R	O	N	G	P	A	S	S	W	O	R	D	K
F	Q	F	H	D	K	L	T	A	Z	A	M	J	X	F	Y
O	F	F	E	N	S	I	V	E	I	E	O	L	L	P	E
R	C	Y	B	E	R	S	E	C	U	R	I	T	Y	A	P
M	A	I	I	R	V	D	X	L	L	Z	D	V	R	S	K
A	J	N	K	I	P	E	R	S	O	N	A	L	K	S	O
T	L	E	F	G	I	D	O	N	E	L	X	J	Y	P	U
I	V	I	M	H	D	K	U	O	P	E	H	O	E	H	B
O	L	O	E	T	D	B	B	S	C	A	M	T	P	R	F
N	H	D	R	S	H	B	F	R	O	S	X	I	K	A	M
R	E	S	T	R	I	C	T	E	D	A	C	C	E	S	S
Z	R	B	A	O	L	I	M	P	F	S	E	I	H	E	O

Cartoon

THE ONLINE SAFETY AWARENESS COMIC SERIES – USEFUL INFORMATION


I am so bored and Mom is busy cooking dinner...
Ooh I have never seen this app before, wonder what it is?
Cool, I can chat with strangers! Maybe make some new friends?
The kid took the bait! Now to get his parent's banking details! Hahaha!
Wait! Do not send that information!
What are you doing on my computer Ryan? Are you about to give my banking details to a complete stranger?

Ryan sits bored in his room wondering what to do.

Ryan notices that there is a dating site open on the laptop.

Ryan explores the application, finds a chat option and starts chatting to a stranger.

The stranger, who is actually a scammer, realises that he is chatting to a young person and tries to get Ryan to send his parent's banking information over the chat.

Crypto steps in to stop Ryan before he sends his mother's banking information.

Practise online safety

- **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.

PROTECT YOUR PERSONAL INFORMATION

Theme 5: Useful Information

Cartoon Questions

1. What is the first thing Ryan did wrong?

....

2. What is the second thing Ryan did wrong?

....

3. Why should you only visit and view age-appropriate websites?

....

4. What do you think would have happened if Crypto did not appear?

....

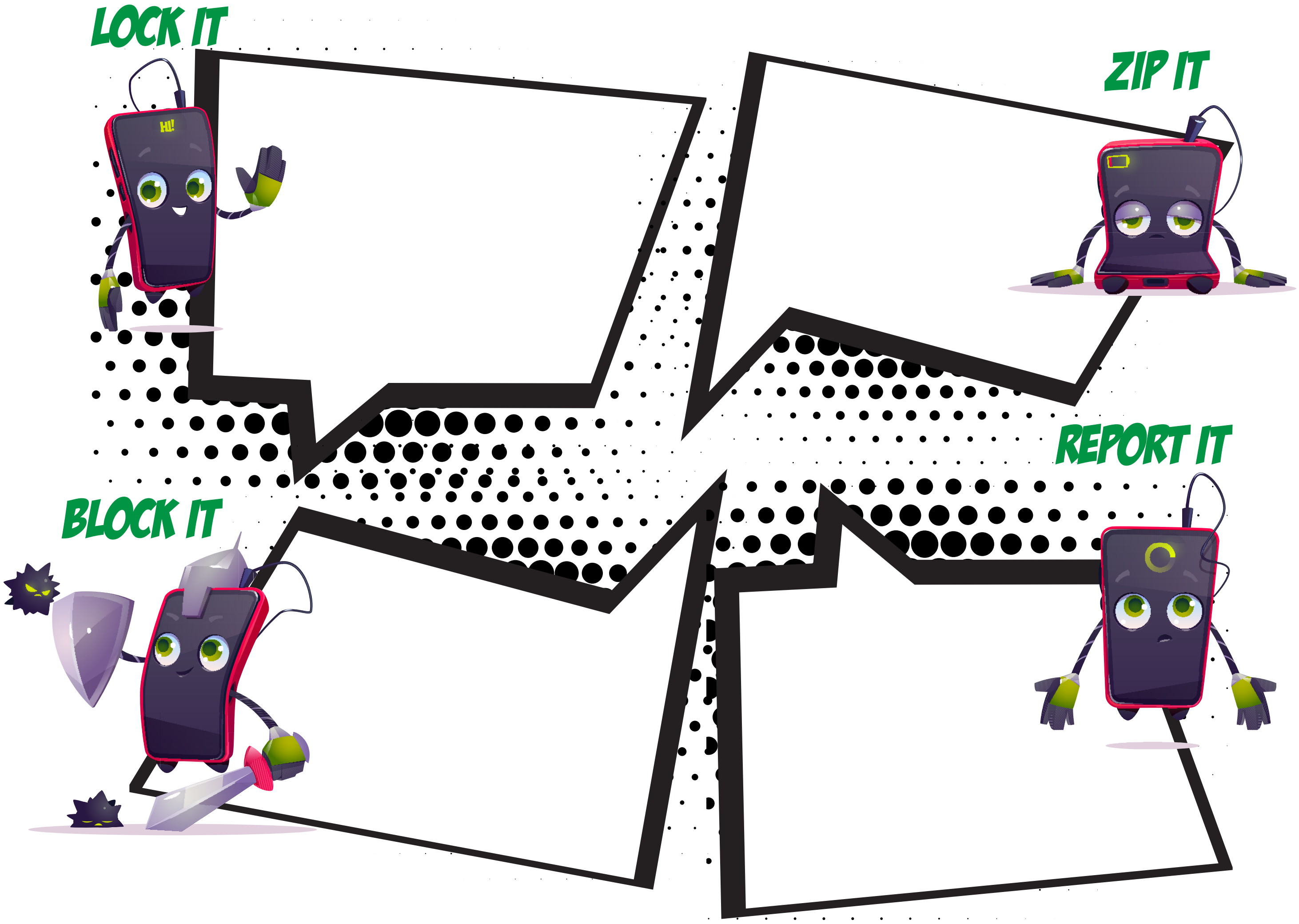
5. What did you learn from this cartoon?

....

Class Discussion

- Have you been a victim of a cyber scam, or know someone that has been a victim? Share your experiences in a class discussion.
- Also, discuss how you or the person dealt with the scam or scammers.

LOOK AT THE ADVICE BELOW: Use the bubbles to write down what, and how you need to lock, block, zip and report!



End of Theme 5

Class Activity and Cartoon Answers

A Trip into Cyberspace - Class Activity - Cartoon

ONLINE
CYBERBULLY
INTERNET
MALWARE
THREATS
CYBER RISKS
PRIVACY
DIGITAL FOOTPRINT
PHISHING
BACKUP
WIFI

1. **What is the first thing Carmen did wrong?**

A: Carmen filled in personal information about herself under the 'about' section on her new social media account.

2. **What is the second thing Carmen did wrong?**

A: Carmen did not update her privacy settings and left her account set to public.

3. **Why is it important to have a responsible digital footprint?**

A: It is important because the content you create, or share online may be archived forever. This information may be visible to anyone who searches for it.

4. **What do you think would have happened if General Flame did not appear?**

A: Subjective.

5. **What did you learn from this cartoon?**

A: Subjective .

Protecting People - Class Activity - Cartoon

1	Cyberbullying	I	Causing harm to a person through the form of electronic text via email, websites, social networking sites or blogs.It is usually done by sending hurtful or threatening messages.
2	Family Safety and Communication	G	Be aware of what you see and hear on the Internet, who you meet, and what you share about yourself. Talk to your parents, use tools to protect your family.
3	Mobile Security	H	The protection of smartphones, tablets, laptops and other portable computing devices, and the networks they connect to, from threats and vulnerabilities associated with wireless computing.
4	Malware	E	Malicious software.
5	PII	B	Personal information, such as your full name, school and home address, and birthday.
6	Phishing	F	The most common type of social engineering attack, used in 90% of data breaches.
7	Social Networking	C	A social networking service is an online platform which people use to build social networks or social relationship with other people who share similar personal or career interests, activities, backgrounds or real-life connections.
8	Mobile Application	D	Referred to as a mobile app or simply an app, is a computer program or software application designed to run on a mobile device such as a cell phone, tablet, or watch.
9	Respect and Ethics	A	A set of values or moral principles that shows how you conduct yourself in cyberspace, and how you show consideration for other people.

1. **What is the first thing Jonathan did wrong?**

A: He was scrolling through a meme website which is not appropriate for his age.

2. **Did Jonathan cyberbully Fatima? If so how?**

A: Yes, by editing the meme to include Fatima's face and sharing it on social media. Fatima did not consent to this.

3. **What did Fatima do that was correct?**

A: Fatima told a teacher about it.

4. **What do you think would have happened if Professor Guardian did not appear?**

A: Subjective.

5. **What did you learn from this cartoon?**

A: Subjective.

Securing Devices - Class Activity - Cartoon - Penalty kicks (Answers)

PASSWORD
TECHNOLOGY
LOCK SCREEN
THEFT
HACKER
SECURITY
THREAT AGENT
SOCIAL MEDIA
CRIMINALS
MOBILE
UNSECURE

1. **What is the first thing Lisa did wrong?**

A: Lisa ignored the software update notification on her phone.

2. **What is the second thing Lisa did wrong?**

A: She accessed a free gaming site on the Internet to download a game instead of downloading it from the cell phone's built-in application store.

3. **Why is it important to ensure that your mobile devices are password protected and encrypted?**

A: If your mobile devices are not password protected and encrypted, anyone will be able to access your information/files stored on the devices. One must protect their personal information, which may be stored on mobile devices.

4. **What do you think would have happened if Techno did not appear?**

A: Subjective.

5. **What did you learn from this cartoon?**

A: Subjective.

Are you ready for a few penalty kicks?

False

Check with your parents before downloading or installing software.

To make sure that the website is secure.

Ensure that your devices' anti-virus and firewall are always kept active and up-to-date.

Class Activity and Cartoon Answers

Smart Apps - Class Activity - Cartoon

1	Downloaded to a mobile device	b	**Social Media**
2	Protection while you browse	e	**Safe Search**
3	Surfing websites	c	**Web Browsing**
4	Playing online	d	**Gaming**
5	Rated according to age	g	**Age Restriction**
6	Apps	a	**Applications**
7	Sometimes referred to as two-step verification	h	**Two-Factor**
8	Setting that shows where you are	j	**Location Settings**
9	Opposite of public settings	i	**Privacy Settings**
10	A dangerous site	f	**Unsecure Site**

A	P	P	L	I	C	A	T	I	O	N	S	O	U	A
W	I	R	M	T	W	O	F	A	C	T	O	R	G	G
P	W	I	T	L	B	P	H	A	S	S	C	T	E	E
O	G	V	I	O	R	X	O	S	L	S	I	R	X	R
Q	A	A	H	C	K	Y	E	S	E	F	A	S	W	E
R	F	C	D	A	S	S	S	J	D	S	L	U	U	S
E	U	Y	U	T	G	A	O	S	E	B	M	K	I	T
F	N	S	E	I	X	S	F	U	M	S	E	E	H	R
T	S	E	T	O	P	E	S	E	S	J	D	F	F	I
P	E	T	K	N	C	N	B	S	S	N	I	Y	K	C
E	C	T	Y	S	N	S	A	I	Q	E	A	Z	U	T
I	U	I	Z	E	O	D	J	P	D	U	A	M	O	I
S	R	N	M	T	L	C	A	Y	O	G	Z	R	S	O
M	E	G	T	T	Y	B	G	X	R	A	F	I	C	N
I	S	S	I	I	H	M	N	I	U	M	G	Y	U	H
W	I	A	F	N	A	E	O	P	F	I	L	P	N	L
T	T	R	L	G	O	C	Q	D	R	N	I	W	M	A
W	E	B	B	R	O	W	S	I	N	G	P	V	U	D

1. What is the first thing Thabo did wrong?
A. Thabo accepted the unknown friend request.
2. What is the second thing Thabo did wrong?
A: Thabo started chatting to the unknown user without verifying the identity of the user first.
3. How can you ensure that a website you are visiting is secure?
A: Ensure that there is a lock icon and an 's' behind 'https' in the top bar (URL bar).
4. What do you think would have happened if The Applicator did not appear?
A: Subjective.
5. What did you learn from this cartoon?
A: Subjective.

Useful Information - Class Activity - Cartoon

Information	-	**Data or facts**
Offensive	-	**Gross or repulsive**
Inappropriate	-	**Wrong, not proper**
Scam	-	**Con or trick**
Strong Password	-	**Secure, good**
Passphrase	-	**Password phrase**
Personal	-	**Own info**
Restricted Access	-	**Access for certain people only**
Rights	-	**Privilege**
Cybersecurity	-	**Staying safe in cyberspace**

I	N	A	P	P	R	O	P	R	I	A	T	E	A	I	R
N	S	T	R	O	N	G	P	A	S	S	W	O	R	D	K
F	Q	F	H	D	K	L	T	A	Z	A	M	J	X	F	Y
O	F	F	E	N	S	I	V	E	I	E	O	L	L	P	E
R	C	Y	B	E	R	S	E	C	U	R	I	T	Y	A	P
M	A	I	I	R	V	D	X	L	L	Z	D	V	R	S	K
A	J	N	K	I	P	E	R	S	O	N	A	L	K	S	O
T	L	E	F	G	I	D	O	N	E	L	X	J	Y	P	U
I	V	I	M	H	D	K	U	O	P	E	H	O	E	H	B
O	L	O	E	T	D	B	B	S	C	A	M	T	P	R	F
N	H	D	R	S	H	B	F	R	O	S	X	I	K	A	M
R	E	S	T	R	I	C	T	E	D	A	C	C	E	S	S
Z	R	B	A	O	L	I	M	P	F	S	E	I	H	E	O

1. What is the first thing Ryan did wrong?
A: Ryan started playing on his mother's laptop without permission.
2. What is the second thing Ryan did wrong?
A. Ryan started chatting to a stranger.
3. Why should you only visit and view age appropriate websites?
A: You should only visit and view age-appropriate websites because you may be exposed to inappropriate content for your age.
4. What do you think would have happened if Crypto did not appear?
A: Subjective.
5. What did you learn from this cartoon?
A: Subjective.

Notes

Notes

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

CYBERSECURITY HUB