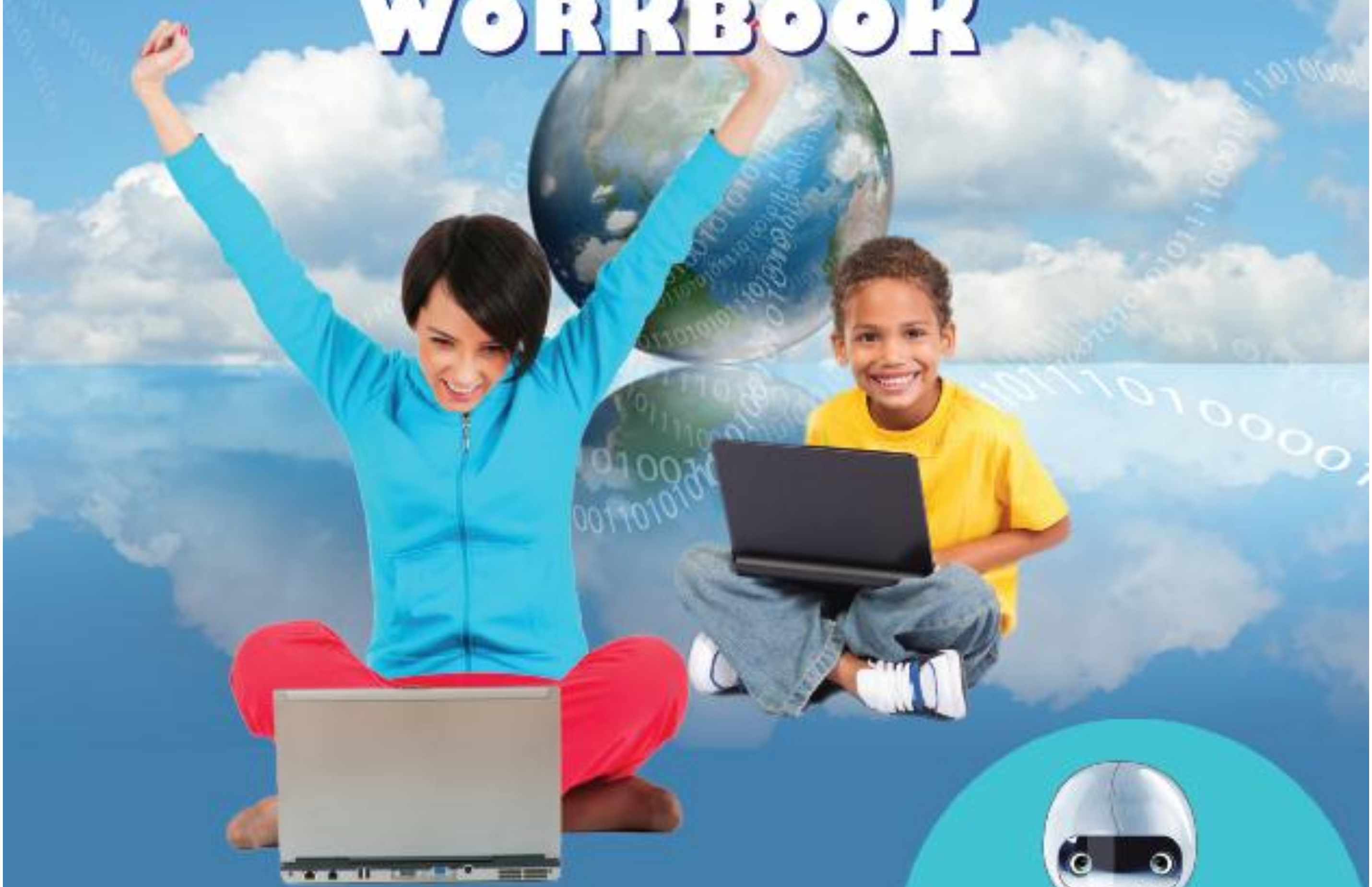
Be aware. Be cyber safe

Children Edition

# CYBER SECURITY AWARENESS WORKBOOK



fpb
Film and Publication Board™

UNISA
college of science, engineering and technology

# Table of Content

**For more information:**

**www.cyberaware.co.za**

UNISA college of science, engineering and technology

# WORD OF WELCOME

We live in a world where technology is integrated into our daily lives. We spend more and more time using the internet for work, education and socialising. Being part of this cyber world is no longer a luxury, but a necessity for many cyber users.

*We are becoming the cyber generation.*

It is, however, important to understand that in order to be part of the cyber generation; one must ensure that all cyber users protect themselves and their personal information. All cyber users should therefore understand the possible cyber threats involved when using cyber devices, such as mobile phones and or tablets connected to the internet.

Ideally, all cyber users should understand the technology they use and how to use it. This research project aims to provide school learners and educators with the essential information on cyber security issues that they should be aware of when using the internet or their mobile phones. To this end, we envisage that this information will contribute to the growth of the cyber security awareness culture in South Africa.

***Prof Elmarie Kritzinger, University of South Africa***

**kritze@unisa.ac.za**

# SOUTH AFRICANCYBER SECURITYACADEMIC ALLIANCE

The South African Cyber Security Academic Alliance or SACSAA (www.cyberaware.org.za) was established in June 2011. The main objective of the SACSAA is to campaign for the effective delivery of cyber security awareness throughout South Africa to all groupings of the population. The founding members of the SACSAA are the University of Johannesburg, the Nelson Mandela Metropolitan University and the University of South Africa (Unisa).

One of the major objectives of the SACSAA in the short term is to organise an annual SA Cyber Security Awareness Day. The Alliance will also invite industry to join as members so that a comprehensive continuous national program of cyber awareness can be operational in SA.

This program will address all potential stakeholders, including:

- school learners on pre-primary level
- school learners on primary level
- school learners on secondary level
- students on tertiary level
- industry
- government
- home user
- anyone using the internet

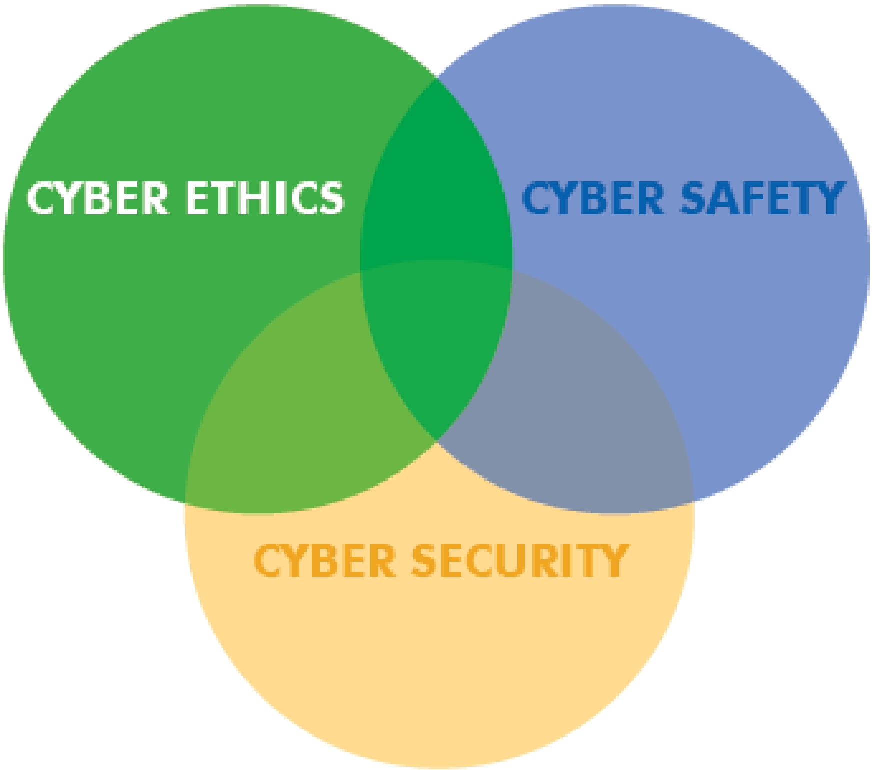
Programs will address the risks of using the internet, including:

- cyber crime
- cyber identity theft
- cyber stalking
- cyber bullying
- internet surfing
- social networks
- internet-based commerce
- other relevant fields

Different mechanisms like this workbook, posters, radio and TV spots, newspaper articles, a dedicated website and more will be used, and where relevant, be available to interested parties. The Alliance trusts that the program over the long term will make South Africa a safer and more secure place from a cyber perspective.

***Prof Basie von Solms, University of Johannesburg***

# CYBERETHICS, CYBERSAFETY, CYBERSECURITY



# CYBERETHICS

The best way to describe ethics is as follows: Treat others as you would like to be treated. Would you like it if someone does to you what you are doing to them?

Cyber ethics, however, is the discipline that deals withwhat is good and what is bad, and with moralduty and obligation as they pertain to the onlineenvironment and digital media. Cyber ethics deals with aspects such as:

- Plagiarism – it is unethical to take another person's ideas or work, and passing it off as your idea, or your work. Would you like it if you do not get recogniton for your effort and all the recognition is given to a person that took your work and passed it off as his or her work?
- Hacking – the unethical practice of gaining access to an environment which you are not authorised to access. Would you like it if a person accesses your private information without your approval?
- Piracy – remember, if you copy  music, software, or videos, you are a thief and you do not subscribe to an honourable code of ethics! Musicians, actors and software developers put a lot of effort into making music, producing a film of developing an application. Would you like it if someone steals the work that you must be paid for and make a living from?
- To post inaccurate or in correct information is unethical behaviour. Would you like it if false information about you is being spread on the internet?

As we can see, cyber ethics is about dealing with things that feel wrong, especially if you consider them from the other person's point of view…

# CYBER BULLYING

Bullying is no longer limited to the bus or the school hallway; kids also use technology to intimidate and harass (to bully) other people.

## What is cyber bullying?

Cyber bullying comes in a variety of forms, which can include embarrassing or cruel online posts, private or embarrassing digital pictures, online threats, harassment and negative comments.

Unfortunately, people do not always treat each other well online. The same rules on how to treat other people are just as applicable in the online environment as they are in the real world.

You or a friend of yours may find that you are the target of cyber bullying. You might be teased or have rumours spread about you on the internet, receive nasty messages or even get threats on your cell phone. It can happen in school during any hour of the day, by people you know and sometimes people you don't know. It can leave you feeling unsafe and alone.

While any age group is vulnerable, teenagers and young adults are common victims.

No one has the right to bully another person. At its most serious, cyber bullying is illegal and can be investigated by the police. Cyber bullying is a growing problem.

## Why has cyber bullying become such a problem?

The internet is fairly anonymous, which is appealing to bullies because their intimidation is difficult to trace. Unfortunately, the internet and e-mails can be used to spread rumours, threats, and pictures very quickly.

# CLASS ACTIVITY 1

## Scenario: Cyber bullies

*Susanne is a new student at Deep Creek Elementary School. She has joined Caroline's fifth grade class a few weeks ago. She is very nice to everyone, but a group of female classmates have started talking behind her back and are excluding her from all activities. Caroline likes Susanne and therefore makes an effort to include her in recess activities. She has even started to e-mail Susanne in the evenings to help plan her upcoming birthday party in two weeks' time.*

*One evening, Susanne sends Caroline an e-mail message in which she is clearly very upset. The girls who had been so unkind to her seemed to be coming around to her birthday party, or so she thought. They had been sending her e-mail messages all night that seemed really nice. So, Susanne decided to invite them to her birthday party. She thought they were trying to be friends and so she innocently responded to the questions they were asking, even though some seemed kind of personal. In addition to asking her home address and who she invited to her party, they also started to ask detailed questions about why her family moved here.*

*Susanne told them that her dad lost his job in their old town and so they moved here because there were better opportunities for him to find a new one in his industry. It turns out the girls were not trying to be her friends at all. They sent out a masse-mail to all of the people invited to Susanne's party saying not to go, that her dad doesn't even have a job and that the party is going to be really lame.*

**Answer the following questions and help Caroline give her new friend Susanne good advice about dealing with these girls.**

### Questions:

1. Are the actions of Susanne's unkind classmates illegal?
2. What are the three steps Susanne should immediately take when receiving these messages?
3. If Susanne doesn't want to tell on the individuals who sent the unkind e-mails, what should Caroline do in this situation? List two steps your team recommends Caroline to take.
4. What is the word used to describe people who use the internet to spread gossip, harass individuals, or ruin someone's reputation?

# LESSON LEARNT

- Cyber bullying is unethical and illegal.
- Stop responding to cyber bullies.
- Block cyber bullies.
- Report cyber bullying immediately.

**What to do if a friend is cyber bullied**

It can be hard to know whether your friends are being cyber bullied. They might keep it to themselves. If they are being cyber bullied, you might notice that they may not chat with you online as much, may suddenly receive many SMSs or be unhappy after they have been on the computer or checked their phone messages. They may stop hanging around with their friends or lose interest in school and social activities.

**Help stop cyber bullying!**

*Stand up and speak out*! If you see or know about cyber bullying happening to a friend, support him/her and report the bullying. You'd want him/her to do the same for you…

*Don't forward* messages or pictures that may hurt or be upsetting to someone. Even though you may not have started it, you will be seen to be part of the cyber-bullying cycle.

*Remember to treat others as you would like to be treated* when communicating online …

# GAMING

Online gaming is fun and interactive. You can play with friends or with people across the world. It often involves interaction with other computers and live players. It's fun for kids to connect with others, but it's important to avoid posting pictures of themselves or releasing other personal information to their fellow gamers. You should also know what to do if another player starts harassing you.

## You must protect yourself

- Do not share any private information such as your cell phone number or physical address with anyone on any site.
- People are often not really whom they say they are.
- Do not choose a username that can be linked to your true identity.
- Do not post an actual picture of yourself in the site; use an avatar instead.
- If another player is making you feel uncomfortable, tell a trusted adult.

# CLASS ACTIVITY 2

## Scenario: Trevor and Mpho's unsafe gaming habits

*Trevor and Mpho have been neighbours since the third grade and are very good friends. They are seriously into video games and their families are constantly telling them to turn the games off and join the rest of the world! Because their parents are good friends, they share information and have the same set of concerns about how "plugged-in" both boys are when they are in the middle of a video game.*

*Trevor's mother complains: "It is like he completely tunes me out!" While Mpho's mother agrees, she is also growing more and more concerned that it is actually physically not good for him to be so plugged into video games, especially when some of them are very violent. Both sets of parents don't want to restrict their teenage sons from using video games, but agree that their current video-game behaviour is unsafe for their wellbeing and something has to change.*

Answer the following questions with regard to Trevor and Mpho's behaviour.

### Questions:

1. Why is the behaviour of Trevor and Mpho not good for their wellbeing?
2. What can Trevor and Mpho's parents do to change their sons' behaviour?

# LESSON LEARNT

- Limit your online play time. Too much online activity can affect your school work and social life and make time for your friends offline.

# ONLINE ETIQUETTE PROTOCOL

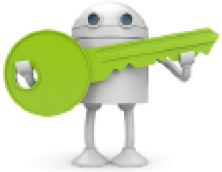
It's important to be kind and polite to others with whom you communicate on the internet – be considerate to fellow internet users. Take some time to think about how your behaviour will affect them.

Sometimes it's easy to forget that the other person you are chatting to online, playing a game with, or sending posts to on his/her profile, is a real person. It's easier to say and do things online that you might not do in "real life". This may hurt that person's feelings or make him/her feel unsafe or embarrassed. It's important to be kind and polite to others online – and to stop and think about how your behaviour will affect them. Remember the golden rule – do to others as you would want them to do to you!

## Good online manners

- Do not say anything that you will not be willing to say to a person face to face.
- Do not hurt someone's feelings.
- Do not use rude language.
- Do not "flame" – thus do not aggravate a situation online.
- Check your spelling.
- Be clear what your subject is about.
- Do not type in uppercase, because then it means you are shouting.

## CLASS ACTIVITY 3



## Scenario

*Sipho and Peter are friends. Sipho has e-mailed the following messages to Peter.*

**Message 1:** Dear Peter
WHY ARE YOU LATE?
Sipho

**Message 2:** Dear Peter
I do not like you anymore!!! You are not a nice person.
Sipho

**Discuss the two messages above in groups.**

### Questions:

1. Do you think Sipho has good online manners?
2. What did Sipho do wrong in each message?
3. Rewrite both messages to adhere to good online manners.

# LESSON LEARNT

- Remember that the person you are chatting to online is a real person.
- Treat other people the way you would like to be treated.
- Think twice before sending any message over the internet.

# TAKE-HOME ACTIVITY

Draw lines to connect the correct terms on the left to the right.

| |
|---|
| Virus |
| Treat people online in the same way you would like to be treated |
| Cyber bullying |
| Social networking |
| Email |
| Identity theft |
| Hacker |

| |
|---|
| Online harassment |
| Facebook |
| Phishing |
| Netiquette |
| Malicious user of computing systems |
| Personal information used without your permission |
| Malicious code |

Uncrable the letters to reveal the correct cyber awareness-related terms:

RVISU

YEDITNIT TTFHE

RBCYELULIBNYG

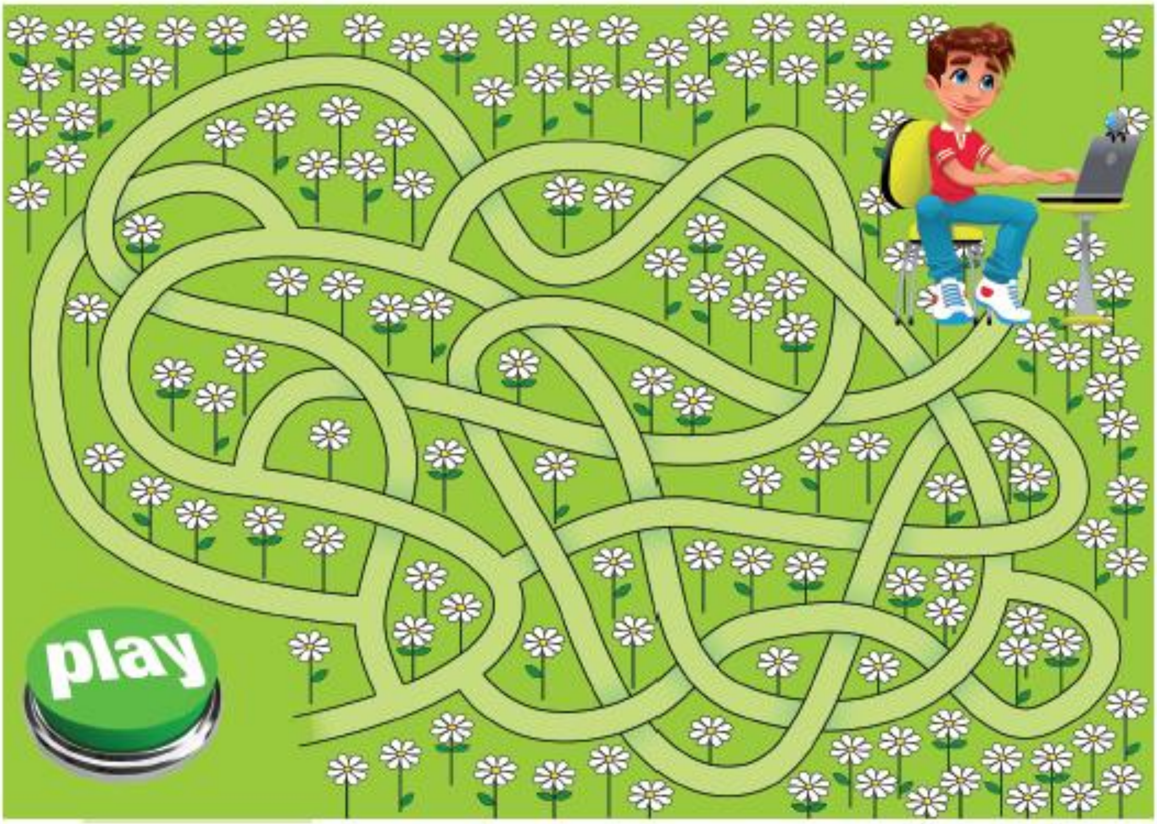
QNEUETTEI

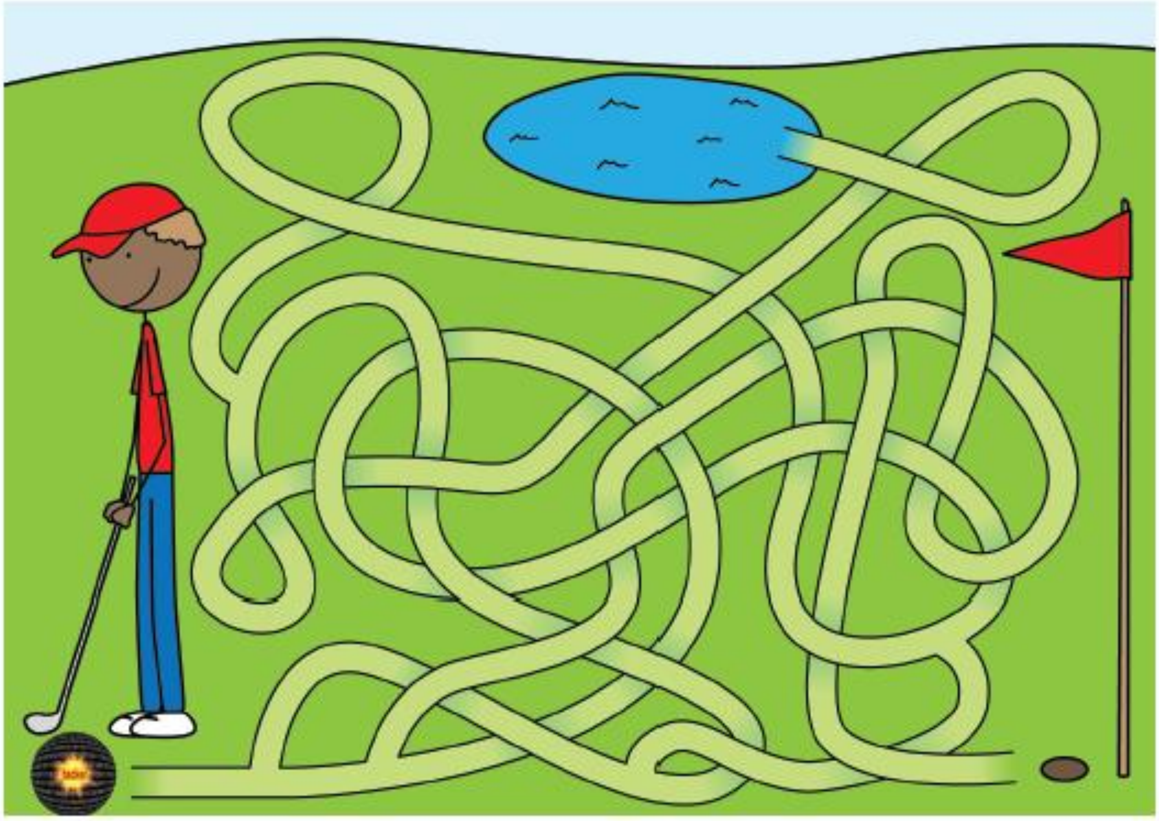
BRECYTSAKLIGN

GPINSHIH

WPAYRES

# Find the paths





# CYBERSAFETY

Whereas cyber ethics focuses on the ability to act ethically and legally, cyber safety addresses the ability to act in a safe and responsible manner on the internet and in online environments. These behaviors can protect personal information and one's reputation, and include safe practices to minimize danger – from behavioural-based rather than hardware-/software-based problems.

In cyber safety, you need to consider aspects such as:

- online predators – people often use cyber space to lure unsuspecting candidates
- cyber stalking – people can follow and harass you online in the same way it is done offline.
- online threats and unwanted communications

The internet is not a game – it is real life!
Learn how to protect yourself against cyber predators, stalkers and bullies.

# UNWANTED COMMUNICATIONS

Unwanted contact is any type of online communication that you find unpleasant or confronting.

Sometimes you can meet someone or see something online that is unpleasant or makes you feel uncomfortable. This could be communication from someone you met online that starts asking personal questions or sends you photos or material that is upsetting or that you don't like. It can sometimes be from someone you know.

The contact can come from online people you don't know or someone you know in person.

## How do I deal with it?

- Tell someone you trust, like your mum, dad or another adult.
- Don't respond and leave the site or chat session.
- Block the contact or remove them from your friends list.
- Don't open messages from people you don't know.
- Keep the evidence. This can be useful in finding the person posting unsuitable material.

# CLASS ACTIVITY 4

## Scenario

*Mpho is in grade 4 in the First Elementary School and is selected for the first rugby team. Some boys at the school feel unhappy about Mpho's inclusion in the team. One afternoon after practice, Mpho receives the follow e-mail.*

*"To Loser. If you do not quit the rugby team, we will hurt you badly. Be wise and hit the road."*

**Discuss in groups the following questions:**

### Questions:

1. How will you feel if you received an e-mail like Mpho?
2. List the potential risks that Mpho faces.
3. What will you advise Mpho to do? Name four (4) things.

# LESSON LEARNT

Talk to an adult, like your parents or a teacher that you trust or to the police if there is any communication which makes you feel uncomfortable.

# OBJECTIONABLE CONTENT

Online, you can be exposed to material that is inappropriate or even harmful to you, whether you are a child or an adult.

It could be through material that is sexually explicit, offensive or violent. It may also be material that contains content that is racist and encourages hatred toward particular groups, or material that encourages unsafe behaviour such as eating disorders. Material that is considered inappropriate can vary depending on family and cultural standards or values.

Watch out for content that is sexually explicit or offensive or even material with a violent theme.

## How do children access inappropriate content?

Children and young people may not deliberately seek out inappropriate content.

They may be inadvertently exposed to such content through otherwise innocuous (i.e. harmless) activities, such as:

- unexpected results from online searches
- clicking on unknown links within websites or e-mails
- clicking on online gaming content or prize offers

In some cases, young people deliberately access inappropriate material, particularly as they move into adolescence. This can be out of curiosity or to share with peers in the "shock value" of the content.

If a website looks suspicious or has a warning page for people under the age of 18 years, **leave immediately. Some sites are not meant for kids.**

**Check** with your parents that your search engine is set to block material that is meant for adults.

Ask your parents to **install internet filter software** to block bad sites. Ask your parents to help you **find safe and fun sites** to use and bookmark for later reference.

# CLASS ACTIVITY 5

## Scenario: Scott remains cyber secure

*Scott is a fourth grade student at Honors Elementary School where his class is doing research in the school's computer lab on ways to stay safe and protected while online. The computers at the school are all connected to the same network, which holds student's personal information.*

*During Scott's research on the internet that day he receives several pop-up ads offering free iPhones with 12months of free mobile services, including text messages if you accept the free trial subscription of "TechIsCool" online magazine. Scott knows the school's Acceptable Use Policy is very clear about not downloading anything on school computers to protect the network. He knows he shouldn't, but he wants an iPhone so badly and doesn't want to miss the opportunity to get the phone for free.*

*Scott clicks on the link offering the free download. He gets suspicious when he starts getting additional pop-up ads asking for detailed personal information. He returns to the StaySafeOnline website and reads all about the potential harm in accepting free downloads. Scott changes his mind, doesn't provide personal information, and returns to his research on cyber security.*

**Answer the following questions:**

### Questions:

1. Scott started to make a potentially big mistake, but wisely changed his mind after reading up on threats from free downloads. List a common threat associated with free downloads.
2. Is there a way to tell if a free download is legitimate?
3. Do you think Scott stopped his actions in enough time to prevent harm to the school's computer and network?
4. List any potential risks that could have happened if Scott had continued to provide personal or school information.
5. List the three important questions Scott should know the answers to before providing any personal information online, especially to some unknown person promising something for free.

# LESSON LEARNT

- Be very careful what you click on when using the internet – not everything on the internet is safe to click on.
- Close a web page or turn off a monitor and call a trusted adult if you are worried about what you see.

# CYBERSTALKING

Cyber stalking is just like stalking in real life, as people can stalk you in the cyber world as well.

## What is cyberstalking?

- A cyber stalker harasses his or her victims online and causes them to feel scared or fearful.
- Online stalkers or cyber stalkers use the internet or another form of electronic communication persistently to cause another person to feel apprehension or fear.
- Online stalking is serious and should be referred to the police or independent legal advisors.

## Why has cyberstalking become such a problem?

When we are connected to the internet, we are not just connected to the friends we know from school or our family in another place, but we are open to a big world that can't be seen, and that world includes some untrustworthy strangers.

**Young children**

Online stalking is less likely among young children as they are not usually involved in online social networking or other websites that involve direct interaction with other people.

For young children, general internet safety tips are a good starting point in helping them to develop appropriate online etiquette and to learn appropriate responses to negative contact from others.

**Older children**

Older children may become more interested in websites and gaming sites that allow direct interaction with others including teens and adults.

## Remember the following 3 Ws:

Who? Who is asking for this information?
*Do we really know them or could they be pretending to be someone else?*
What? What are they asking for?
*STOP if it is your personal information.*
Why? Why do they need it?
*Most people don't NEED to know your personal information. You should always tell your parents if someone is asking for it. They will know whether or not you should give it out.*

# CLASS ACTIVITY6

## Scenario:

*Julie loves to use Club Penguin and Webkinz. Her parents allow her to play the games as long as they are in the room monitoring what she is doing while playing. One day, while playing online, Julie receives a message from one of the other (characters) asking how old she is and what school she goes to. The character is dressed as a girl (character) but Julie does not know her. Fortunately, Julie knows the rules about providing personal information to anyone online. So, with her parents sitting next to her, she blocks the person.*

*Julie's parents praise her for remembering to never give out personal information.*

**Answer the following questions.**

### Questions:

1. Why do you think this could have been a dangerous situation?
2. How would Julie know if this was a person she knew in real life, like a friend from school?
3. Are there any other steps Julie and her parents could take to be any safer?

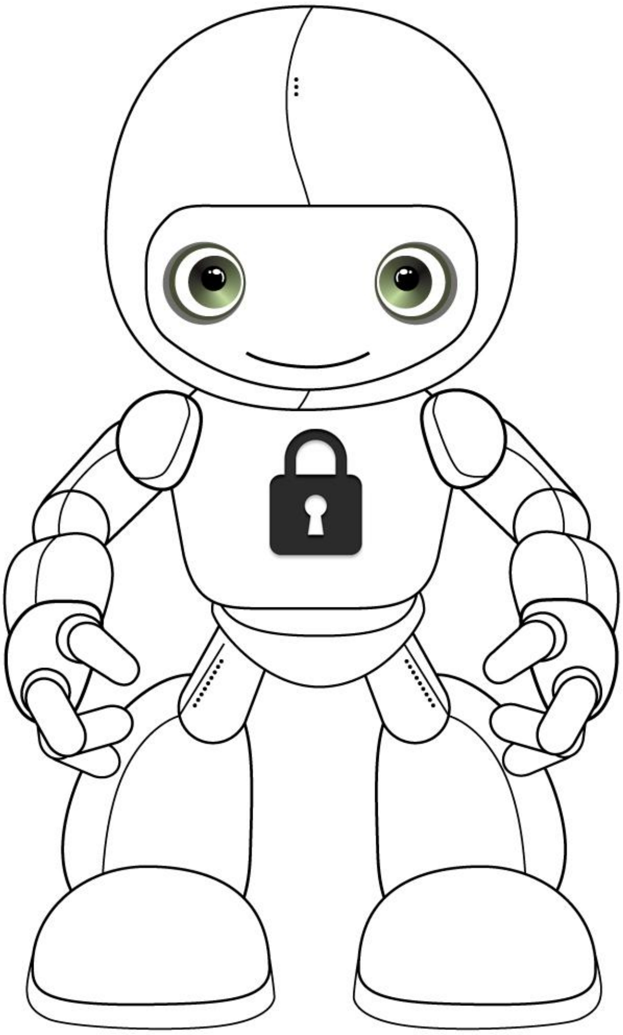
## LESSON LEARNT

NEVER give out any personal information such as a telephone number, address, of information which can be used to locate you by anyone on the internet.

## TAKE-HOME ACTIVITY

Colour in and cut out the attached picture of the computer with the pledge that you promise to never give out personal information or talk or meet with anyone you meet over the internet.

# MY INTERNET SAFETY PLEDGE



**I promise to never give out my personal information over the internet unless my parents say I can.**

**I promise to remember that people can pretend to be someone they are not over the internet.**

**I promise to tell my parents if someone I don't know tries to contact me over the internet or asks me to tell them my personal information.**

***___________________________________________**
**(My name)**

***___________________________________________**

**(Parent/Guardian Signature)**

# Complete the crossword puzzle

Everybody should be (1 down)_________ of cyber (2 across)__________ and how to (3 down) ________ themselves.

(4 across) _________ is the discipline dealing with what is good and bad.

Never reveal your (5 across)________ when playing online games.

Use a strong (6 down) _________ for your gaming accounts.

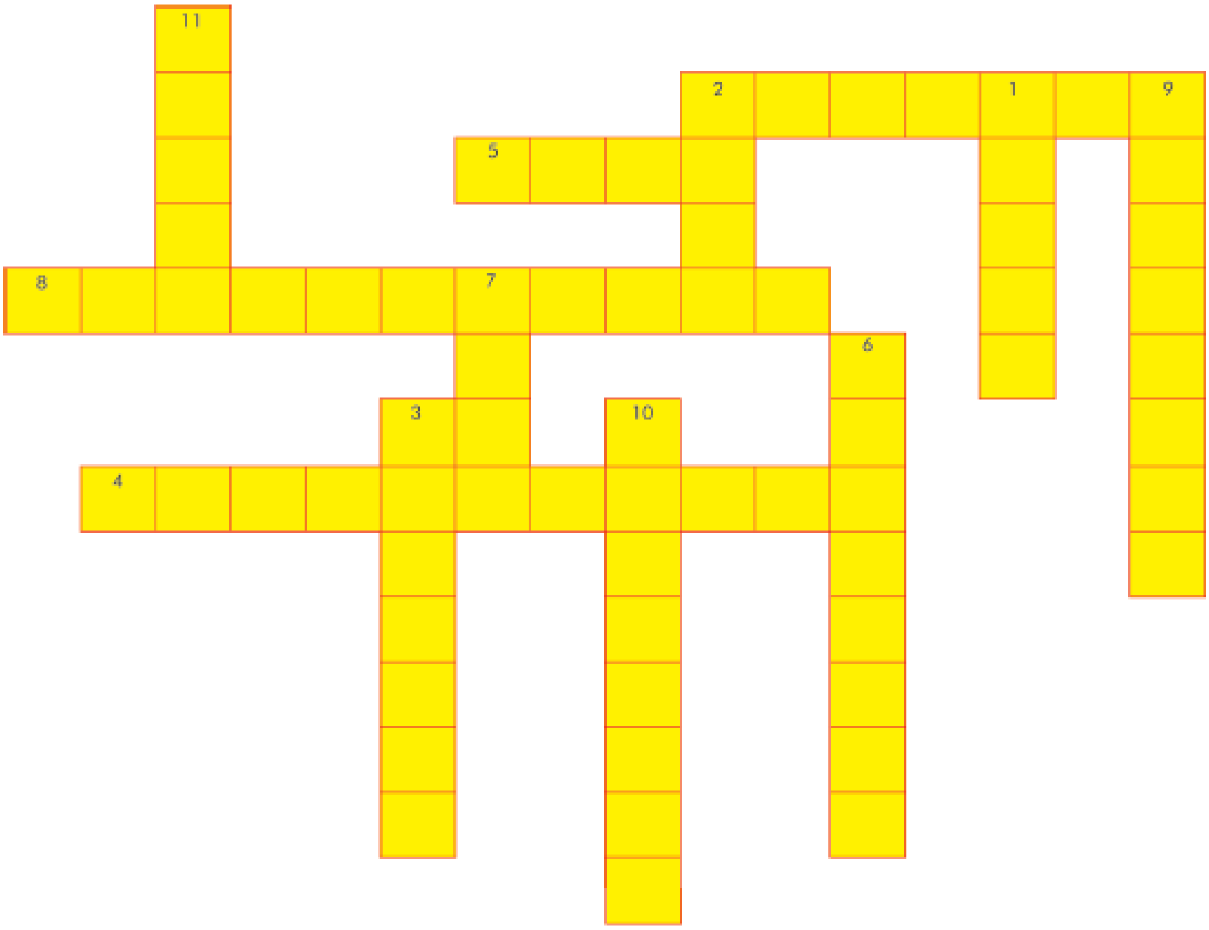
Cyber safety addresses the ability to act in a (7 down) _______ and (8 across) _________ manner.

Beware of online (9 down) _____________ .

When someone makes you feel uncomfortable online (2 down) ________ an adult.

(10 down) _______ is the use of email to encourage individuals to reveal financial details.

Instal antivirus software to protect your computer from a (11 down)__________.



# CYBERSECURITY

Cyber security is defined to cover physical protection (both hardware and software) of personal information and technology resources from unauthorized access gained via technological means. In contrast, most of the issues covered in cyber safety are steps that one can take to avoid revealing information by social means. Cyber security topics may include the following:

- Identity theft – it is possible for bad people to steal the information that you use to identify yourself online – in effect the person can then become you and masquarade as you online.
- Phising – beware that you do not share any personal information or banking details online. Certain e-mails and websites lure you into supplying personal information, which is known as phising attempts.
- Be very careful of anybody promising you money – if you did not enter the national lottery, how can you have won any money from them?
- Do not send along chain letters – they clog the e-mail system.

You should protect your computer and employ good computer “hygiene”. Much like you are taught to wash your hands to avoid disease computer if you do not follow a handful of computer basics.

# IDENTITYTHEFT

Identity theft is a specific type of fraud, which involves stealing money or gaining other benefits by pretending to be someone else.

Identity theft is when your personal information is used without your knowledge or permission. This can take a variety of forms and, in the worst case; it can involve criminalizing your information to steal money from you or to open bank accounts or credit cards in your name. While this may not seem a problem if you don't yet have a credit card, it might damage your chances of getting one when you're older.

Personal information can be accessed from your computer or at a public computer terminal. With sufficient information, criminals can make credit card purchases, apply for loans or transfer money directly from your bank, while pretending to be you.

Criminals use many methods to gather personal information, including sending viruses and spam, and setting up fake websites. You can also have your identity "stolen" if someone uses your personal information to impersonate you online. They might pretend to be you, make a fake profile of you or hack into your actual profile!

Identity theft can be devastating, both financially and emotionally.

## How can I protect my identity?

- Ask your parents to help you to install antivirus software– the correct version for your internet browser– and remember to activate your computer's firewall.

- Tell a trusted adult before posting any personal information online and be very careful when entering a competition.

## Why is it dangerous to post personal information on the web?

This sort of information can be used to identify or locate where you live or go to school.

# CLASS ACTIVITY 7

## Scenario

*Hanifa received the following e-mail:*

*Dear Hanifa,*

*Hope you are still enjoying school. I am also in your school and was selected for the rugby team this year. Do you want to meet this weekend? Where do you live? Can we meet at your place?*

*See you soon,*

*Peter*

Hanifa does not know Peter and she is not sure if he is in her school or not.

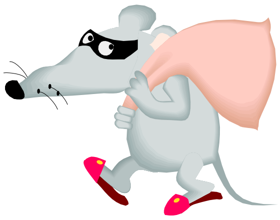
**Discuss the following questions in groups.**

**Questions:**

1. Must Hanifa answer the e-mail? Why?
2. Name another way in which you can compromise your identity.

## LESSON LEARNT

Always ask permission to give out private information in cyber space.



# VIRUSES

Did you know that a little bad program called a virus can harm a computer?

Viruses infect computers when infected files are downloaded onto a vulnerable computer by vandals. These people only want to damage computer programs and files, sometimes slowing down the computer. Some smarter viruses may not cause damage straight away, but lurk in the shadows waiting for the right moment.

Virus files can make a computer stop working.

## How can I protect my computer against viruses?

- Do not connect unreliable USB memory sticks to your computer.
- Be very cautious when activating attachments found in e-mails.
- Ask your parents to install antivirus software.**Antivirus software** should be set to automatically scan all incoming and outgoing e-mails and any devices that are intermittently connected to a computer, such as a memory stick, a music player, digital camera or other USB devices. Set the software to automatically check for updates when connected to the internet.
- **Use a firewall and make sure it is turned on.** A firewall is your computer's first line of defense against intruders. Firewalls can block all traffic between your network and the internet that is not explicitly allowed, preventing unauthorized access to your data. A firewall should be used in conjunction with antivirus and antispyware software.
- **Manage e-mails safely.** Delete suspect e-mails immediately. If you do open an e-mail that seems suspect, don't click on any links in the e-mail. All e-mail attachments should be scanned by antivirus software before being opened. Antivirus software can be set to do this automatically.
- Use spam filtering software to manage unwanted e-mails and report spam to the authorities.
- **Use safe internet browser settings.** When browsing the web, creating documents, reading e-mails and playing games, using a limited permission account can prevent malicious code from being installed onto your computer. A "limited permission" account is an account that does not have "Administrator" status.
- **Keep up to date with security patches.** Most operating systems are supported by automatic updates ("security patches") that fix vulnerabilities found in important software components. You should either use the "automatic update" option, or subscribe to a security-related mailing list and install these patches when necessary.

# CLASS ACTIVITY 8

## Scenario: Jabu and the bad virus

*Jabu was using the internet on his family's home computer to research a school project on dolphins that is due the next week. He just finished finding the perfect article to add to his research and was about to log off. Before shutting down, Jabu decides to quickly check his e-mail account. In his "Inbox", Jabu sees two messages including one from NO1GRANDPA@YAHOO.COM, which he recognizes as his grandfather's e-mail address, and another fromSWEEPSTAKES@HOTMAIL.COM with a subject line that reads **"YOU'VE WON$5,000".***

*Jabu skips his grandfather's e-mail and quickly opens the sweepstakes e-mail to collect his prize. After doing so, Jabu receives a message instructing him to provide personal information to verify his identity. He provides his full name, date of birth, home address and phone number. He hits submit and instantly starts receiving messages saying his computer has been infected by a virus.*

*Jabu panics because he doesn't want to get into trouble. He quickly logs off, shuts off his computer, and goes to bed, hoping his parents won't know what happened in the morning.*

### Questions:

1. There are four major mistakes Jabu made in this scenario. Can you identify Jabu's mistakes?
2. Can you list the thoughts and actions Jabu should have taken after each of his errors that would have prevented further damage.

## LESSON LEARNT

Never open or respond to unwanted e-mails or messages.

# PHISHING

Phishing is the use of a website, e-mail or SMS to encourage individuals to reveal personal details such as financial information like credit card numbers, account names, passwords or other personal information. Scams are ways of obtaining information or money through false means. Spam is an unsolicited commercial electronic message.

Phishing messages can look like genuine messages from a real bank, a telecommunications provider, an online retailer or a credit card company.

Some tips to manage and identify phishing scams:

Avoid giving out your e-mail address or mobile phone number publicly and check that children aren't giving out details.

Check the terms and conditions of anything you and your children sign up for – for example, are you consenting to receiving commercial messages?

Do not respond to unknown SMSs asking you or your children to make contact and provide cash or financial information. If a phone or e-mail contact seems unusual, especially if money is involved, hang up or do not reply.

If you receive a message from a legitimate business, for example a financial institution or shop, but do not want to receive messages from that organization, you can unsubscribe through an e-mail link or SMS "STOP".

Install and update antivirus and other e-security software to restrict unauthorized access to data on the home computer and protect that data from corruption.

Ensure that security features including a firewall are turned on, set to automatic scan and updated regularly to protect against the latest risks.

## LESSON LEARNT

- Delete and do not respond to suspicious e-mails.
- Do not provide passwords or any personal information in an e-mail.
- If you receive an attachment from someone you do not know or an unexpected attachment from known source, do not open it.

# CLASS ACTIVITY 9

## Search for and circle the cyber awareness terms

Look for the following cyber awareness terms in the block below and circle them. The words can be in any direction (from left to right, from top to bottom, from bottom to top or diagonal):

CYBER STALKING
HACKING
CYBER ETHICS
VIRUS

HARASSMENT
COPYRIGHT
CYBER SECURITY
SPOOFING

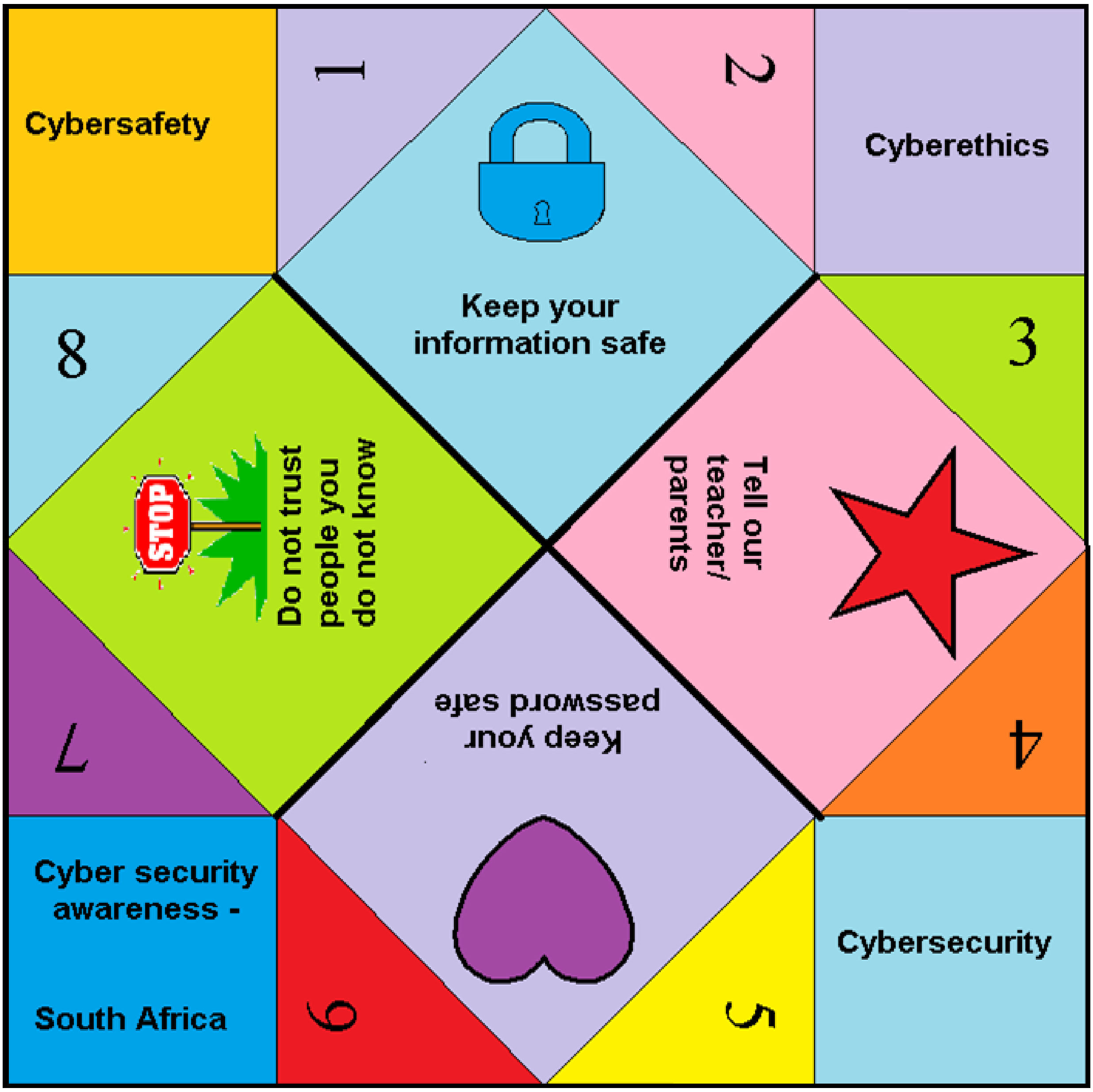
PLAGIARISM,
CYBER SAFETY,
PHISHING
SPYWARE

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

# TAKE-HOME ACTIVITY

**Cut out and fold:**

Cut out


Cybersafety
1
2
Cyberethics
Keep your information safe
8
3
Do not trust people you do not know
STOP
Tell our teacher/ parents
7
4
Keep your password safe
Cyber security awareness - South Africa
6
5
Cybersecurity

Cut out the square.
Fold the paper from corner to corner to make a triangle.
Fold the triangle from corner to corner again, making a smaller triangle.
Unfold.
Fold the four corners to the centre of the square.
Turn the paper around.
Fold the four corners to the centre of the square.
Push the four corners of the square into the centre and then slide four fingers into the flaps of your fortune teller.

Cut out

-- The end ---

## ANSWERS TO CLASS ACTIVITY 1

### Question 1

Not only is cyber bullying extremely unethical, but laws also protect students from being bullied either in person or online. Because of certain serious consequences that have resulted from cyber bullying, local law enforcement as well as federal authorities can now prosecute students and families who cyberbully people.

### Question 2

1. Stop responding immediately to anyone online who makes you feel uncomfortable or who you don’t trust and know well in person.
2. Block this person from ever contacting you again.
3. Tell your parents or guardians, and in this case, because it involves classmates at school, tell your teacher.

### Question 3

Caroline could tell her own parents about the incident and inform her teacher at schools she can avoid future situations such as these with this group of unkind girls.

### Question 4

Cyber bullies

## ANSWERS TO CLASS ACTIVITY 2

### Question 1

Trevor and Mpho are neglecting their “real worlds” by gaming so often. They don’t have time for friends and family.They are also exposed to violence which can lead to unaccepted behaviour.

### Question 2

Trevor and Mpho’s parents should limit their son’s exposure to violent games and make sure what they are playing is age appropriate. They should monitor how much time they spend playing games and set rules with regard to the maximum time they are allowed to play online games during a week. If Trevor and Mpho don’t want to be monitored, then they should be more responsible about how much time they spend playing games.

## ANSWERS TO CLASS ACTIVITY 3

### Question 1

No, Sipho definitely does not have good online manners.

### Question 2

In the first message Sipho used capital letters. This is inappropriate because it means that he is shouting. In the second message Sipho hurts Peter’s feelings by telling him that he doesn’t like him anymore and that he is not a nice person.

### Question 3

Message 1: Dear Peter
Why are you late? I am worried.
Regards, Sipho
Message 2: Dear Peter
I do not understand why you did not come. Please let me know.
Regards, Sipho

## HOME ACTIVITIES

### ACTIVITY 1

| | |
|---|---|
| Virus | Malicious code |
| Treat people ... | Netiquette |
| Cyber bullying | Facebook/Online harassment |
| Social networking | Phishing |
| Email | All |
| Identity theft | Personal information used |
| Hacker | Malicious user |
| | |

### ACTIVITY 2

| |
|---|
| Virus |
| Identity theft |
| Cyber Bullying |
| Copyright |
| Netiquette |
| Cyber Stalking |
| Phishing |
| Spyware |

## ANSWERS TO CLASS ACTIVITY 4

### Question 1
My feelings would be hurt and I will feel upset and scared.

### Question 2
The children who wrote the message could hurt Mpho.

### Question 3
Sipho should tell someone he trusts, for example his parents or his rugby coach.
He should not respond to the e-mail.
He should keep the e-mail as evidence to show to a trusted adult.
Sipho should block the contact.

## ANSWERS TO CLASS ACTIVITY 5

### Question 1
It makes your computer vulnerable to a virus.

### Question 2
It is hard to verify if a “free download” is legitimate. Here are a couple of possible tips:
Ask yourself if the free offer is from a reputable company. If so, verify with the company by phone that they are truly making this offer.
Ask yourself if this offer is too good to be true. If it sounds too good to be true, it probably is. Your antenna should go up that his may be a phony attempt to do harm to you or your computer.

### Question 3
It is hard to say. By simply accessing the link to accept the free download, it is possible that he made the school network security vulnerable.

### Question 4
Scott could have compromised his own protection as well as that of his classmates by allowing private information to be passed through the school network. He could also have been charged with vandalizing school property if his actions damaged the school’s computer.

### Question 5
Who is asking for the personal information?
What are they asking for?
Why do they need this information?

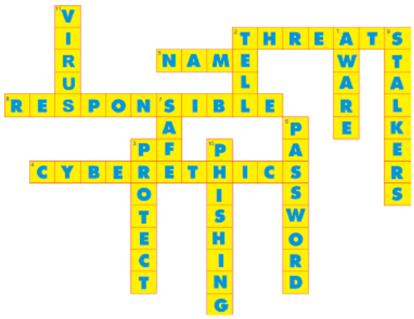
## ANSWERS TO CLASS ACTIVITY 6

### Question 1
If Julie posted her personal information on the web, the “character” could use her information to stalk her.

### Question 2
Julie would not know if the person is someone she knows in real life.

### Question 3
Julie should maybe not play those games for a while so that the potential stalker loses interest.

Cross word



## ANSWERS TO CLASS ACTIVITY 7

### Question 1

No, because she does not know this person and she also does not know if he is who he claims to be.

### Question 2

You can compromise your identity when you enter personal information on a web site such as for a competition entry.

## ANSWERS TO CLASS ACTIVITY 8

### Question 1

**Jabu's four mistakes**:

1. He opened an e-mail from an unknown source.

2. He took the bait in this phishing scam that promised something too good to be true.

3. He provided personal information to an unknown source.

4. He was not honest to his parents or guardians about the negative experience he had online that compromised the family computer's security.

### Question 2

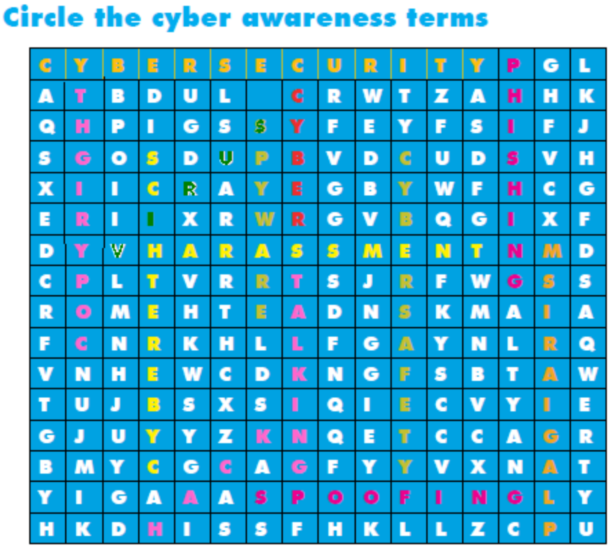
**What should Jabu have done?**

1. Jabu's first step should have been to delete the e-mail from the unknown source without opening it.

2. After opening the fraudulent e-mail, Jabu's knowledge of the WWW Decision Tool should have made him suspicious when the unknown source started asking for personal information. He could have then stopped, deleted the e-mail, told his parents and even reported the incident to the Federal Trade Commission.

3. The most important step Jabu should have taken is that, after making the mistake that caused the virus, Jabu should have told his parents about the incident so they can restore their computer's security and prevent further loss of private information.

## ANSWERS TO CLASS ACTIVITY 9



Circle the cyber awareness terms

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

**REFERENCES**
**http://www.staysafeonline.org/content/privacy-policy**

Reservation of Rights: All Contents (including, without limitation, the graphics, icons, and overall appearance of the web site and the Contents) are the property of the Alliance or its affiliates. Neither the Alliance nor its affiliates waive any of its proprietary rights therein including, but not limited to, copyrights, trademarks and other intellectual property rights. This web site and the Contents are intended only for the individual, non-commercial use of web site users. No user of this web site may resell, republish, print, download, copy, retransmit or display (by use of an html "frame" or otherwise) any portion of this web site or the Contents without the prior written consent of the Alliance, except that reasonable copying or printing of the Contents for individual, non-commercial use is permissible where permitted by law.

**http://www.cybersmart.gov.au/Legal/Copyright.aspx**

Copyright notice© Commonwealth of Australia

The materials on this website constitute Commonwealth copyright. Unless otherwise indicated, you may download, store in cache, distribute, display, print and reproduce materials on this website in unaltered form only (retaining this notice, and any headers and footers that appear with the original materials) for your personal, non-commercial use or use within your organisation. Apart from any use permitted under the *Copyright Act 1968*, any relevant Creative Commons licence (see below) or under this copyright notice, all other rights are reserved.

If you have questions about the use of these materials or would like to apply for permission to use materials on this website, which is beyond what is permitted under this notice please contact:

Manager, Communications and Publishing
Australian Communications and Media Authority
PO Box 13112 Law Courts
Melbourne Vic 8010

Tel: 03 9963 6800
Fax: 03 9963 6899Email: candinfo@acma.gov.au
Website: www.cybersmart.gov.au

**http://cybersmart.org/legal/**

Terms and Conditions

Acceptance of Terms of Use

Please read the following terms and conditions carefully before using The Cyber Smart! Education Company site ["Cyber Smart!"]. By accessing and using the site, you are agreeing to these terms and conditions. If you do not accept these terms and conditions, do not use Cyber Smart site.

Users of this Site are responsible for their use. Cyber Smart does not assume any liability regarding the use of this Site by any user. At any time and in our sole and absolute discretion, Cyber Smart may amend, modify, add or delete any content or any portion of this Web site, including the site in its entirety.

Permissions

The contents of The Cyber Smart! Education Company site may not be sold by any party, nor otherwise distributed in any manner that results in any direct or indirect charge or expense to the user thereof. Information provided is intended for instructional and informational uses and purposes only and is to be distributed free of charge except in the specific case of Cyber Smart! Online Workshops which are sold.

All content of this Web site, and any materials downloaded from it, but excluding materials downloaded from any third party linked site, are copyrighted © All rights reserved.

Copyright and Proprietary Rights

All contents of this Web site, its text, graphics and design elements, any materials downloaded from this Web site (but excluding materials downloaded from linked Web sites) and any print (and other media) versions is proprietary to The Cyber Smart! Education Company including the copyright and all rights under copyright therein. The Cyber Smart Student Curriculum and Cyber Smart! Online Workshops are protected by United States and International Copyright laws.

**www.safesurfingkids.com**

# Cyber Security Awareness

www.cyberaware.org.za