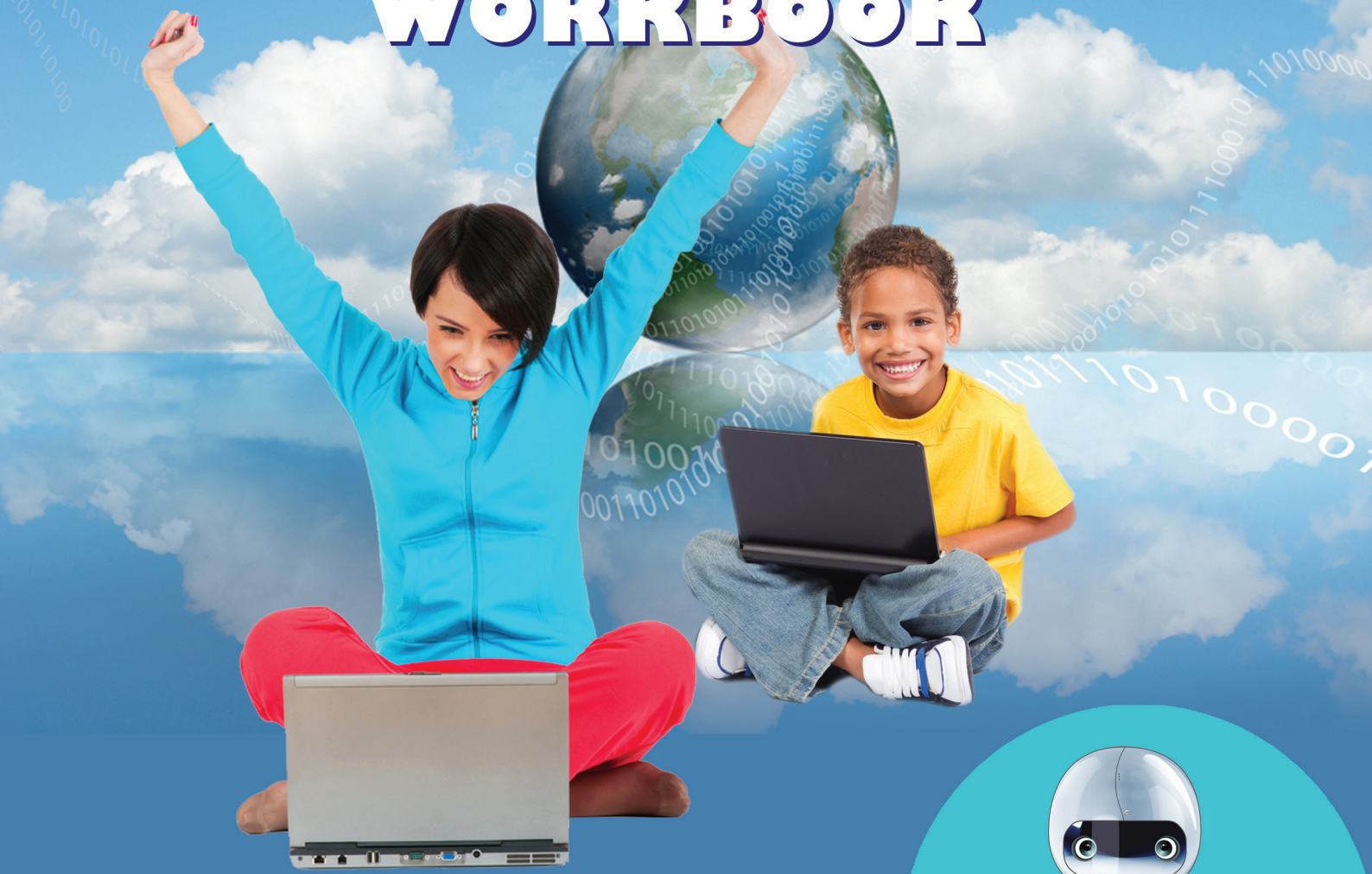
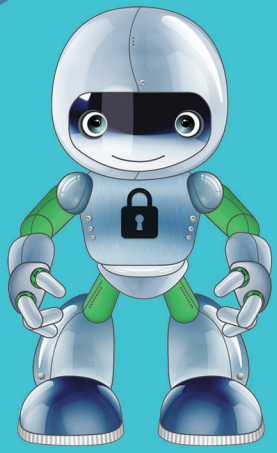
Be aware. Be cyber safe

# CYBER SECURITY AWARENESS WORKBOOK





SACSAA
South African Cyber Security Academic Alliance

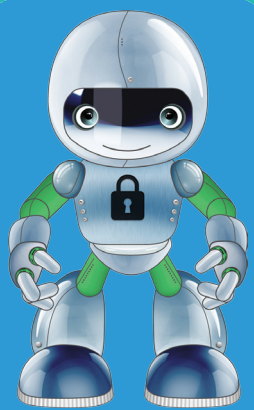
NRF

Microsoft

UNISA | college of science, engineering and technology

# CONTENT





# WORD OF WELCOME

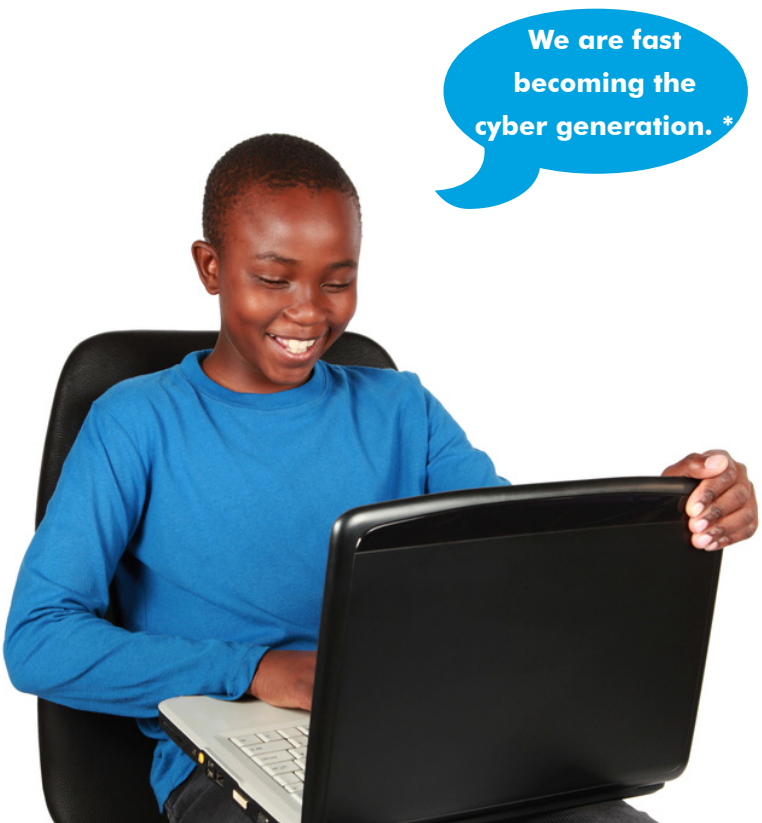
We live in a world where technology is integrated into our daily lives. We are spending more and more time using the internet for work, education and socialising. Being part of this cyber world is no longer a luxury, but a necessity for many cyber users.

As part of the cyber generation, however, it is important that all cyber users protect themselves and their personal information. All cyber users should therefore understand possible cyber threats involved when using cyber devises, for example PCs and mobile phones. *

This Cyber Security Awareness Workbook was created to provide school learners and educators with essential information on cyber security issues they should be aware of when using the internet or their mobile phones. We trust that this information will raise awareness of cyber security in South Africa and help all cyber users to understand the technology they are using and to use it safely.

I extend special thanks to all who were involved in the process of creating and distributing this Cyber Security Awareness Workbook.

*Prof Elmarie Kritzinger*
*University of South Africa*
Kritze@unisa.ac.za



# South African Cyber Security Academic Alliance

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

One of the main short-term objectives of SACSAA is to organise an annual South African Cyber Security Awareness Day – the first being planned for October 2012. The Alliance will also invite people from industry to join as members so that a comprehensive, continuous national programme of cyber awareness can become operational in South Africa.

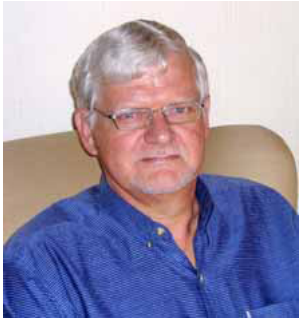
This programme will address all potential stakeholders, including the following:

- school learners at pre-primary level
- school learners at primary level
- school learners at secondary level
- students at tertiary level
- people from industry
- people in government
- home users
- anyone using the internet

Programmes will address the risks of using the internet, including the following:

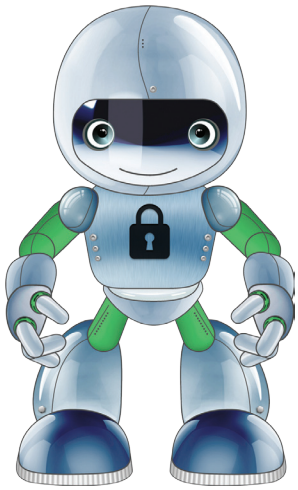
- cyber crime *
- cyber identity theft
- cyber stalking
- cyber bullying
- internet surfing
- social networking
- internet-based commerce
- other relevant fields

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



*Prof Basie von Solms*
*University of Johannesburg*

This Cyber Security Awareness Workbook is an attempt to address security issues surrounding the use of technology instruments such as cellphones and computers. This is an important contribution to the burgeoning body of literature on cyber security both in South Africa and the rest of the world. It should serve as a valuable tool for concerned adults to enhance the safety and wellbeing of young people as they navigate their increasingly technological worlds.



Nearly every day our nation is discovering new threats to and attacks on our South African networks. Inadequate cyber security and loss of information will continue to inflict significant damage to South African national and economic security if left unchecked. There are many "bad actors" out there, and many types of these bad actors. There are criminals, there are *organised crime groups, there are hacktivists, and there are those committing economic espionage or military espionage.

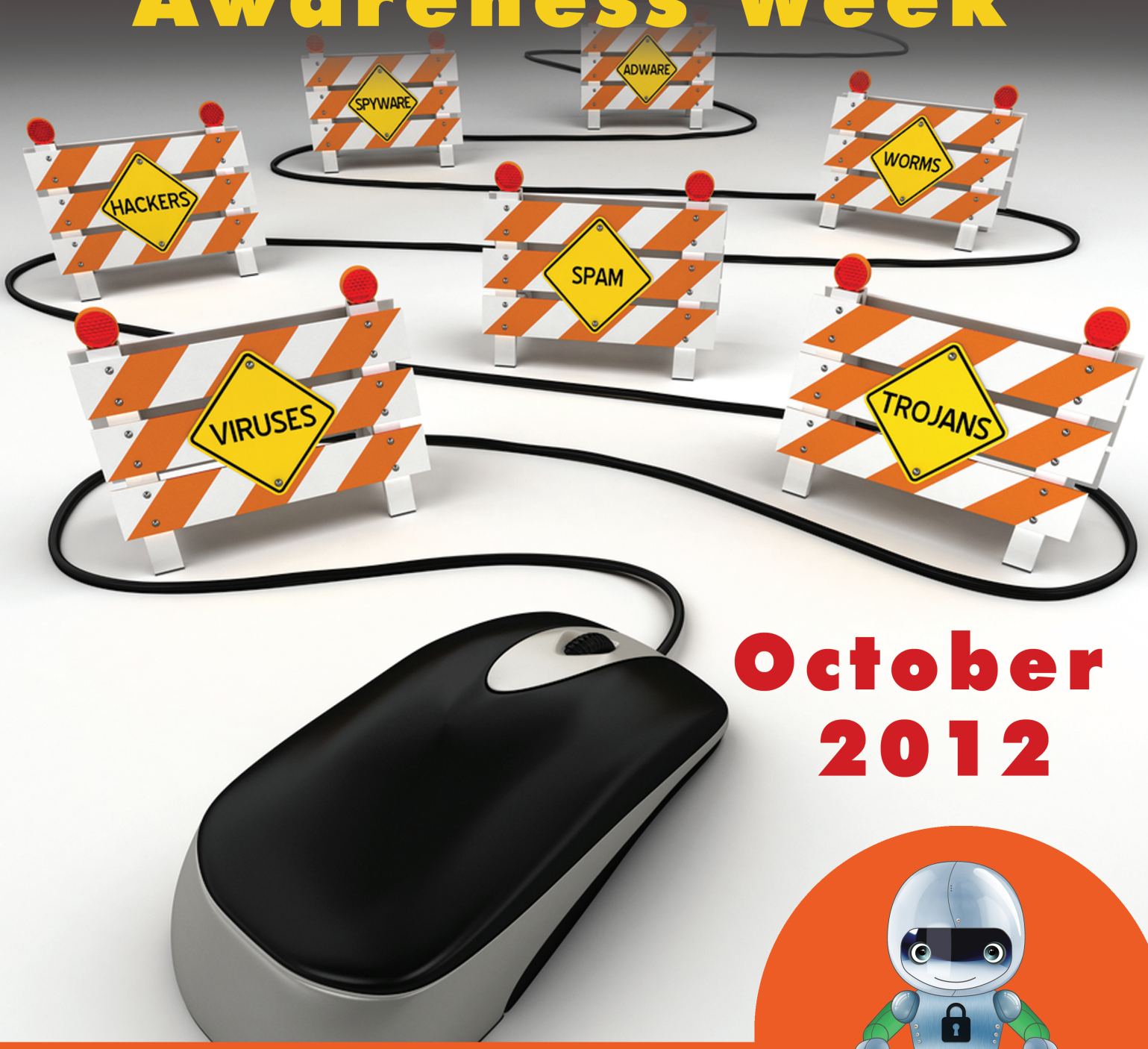
Other bad actors are bullies, notorious for tormenting their victims face to face — at school, on the playground, on sports fields. Cyber bullying (or online bullying) has opened the door to 24-hour harassment using computers, cellphones, gaming consoles or other internet-enabled means. These bullies can remain anonymous and can continue to intimidate, harass and belittle others.

This workbook covers topics relating to cyber ethics, cyber safety and cyber security, and will go a long way toward addressing issues affecting us and, more importantly, our children/teenagers. Cyber safety is about establishing trust by creating alignment: alignment between social forces, political forces, economic forces, and IT products and services. If you don't create that alignment, you may end up with great technology that is economically unsustainable or objected to by many. To prevent innocent internet users from becoming victims of cyber attacks, an intensive awareness campaign is necessary to educate novice internet and technology users with regard to basic security. This workbook will go a long way toward addressing part of this awareness.

*Dr Khomotso Kganyago*
*Chief Security Advisor*
*Microsoft South Africa*

Be aware. Be cyber safe

# National Cyber Security Awareness Week




## October 2012



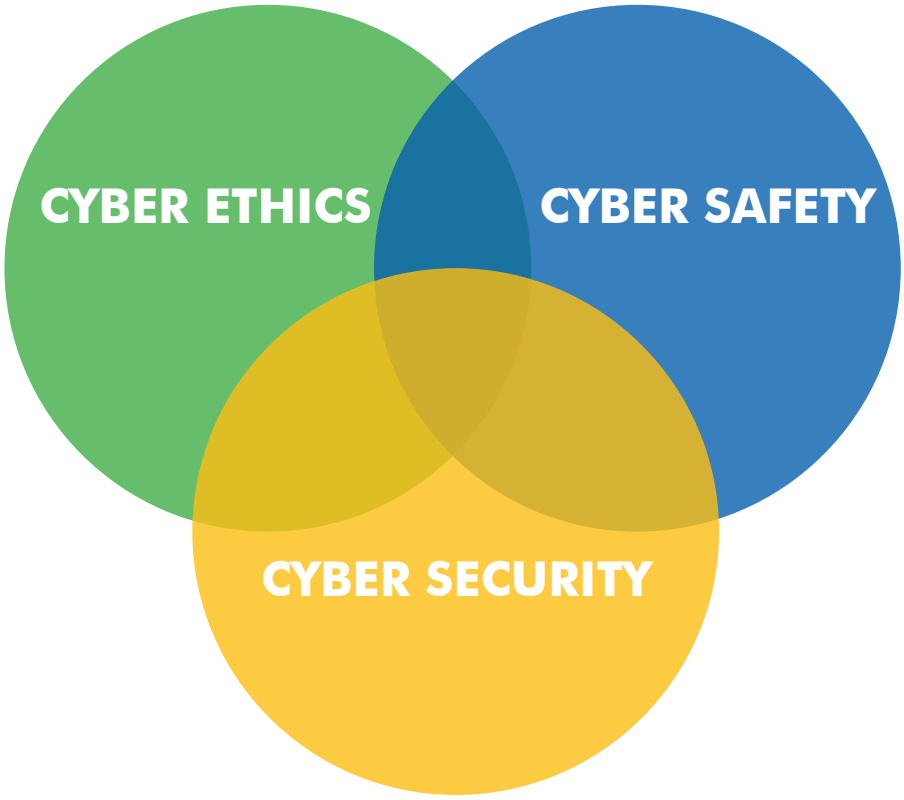
SACSAA South African Cyber Security Academic Alliance

NRF

Microsoft

UNISA college of science, engineering and technology

www.cyberaware.org.za




# CYBER ETHICS


Cyber ethics is the discipline that deals with what is good and what is bad, and with moral duty and obligation as they pertain to the online environment and digital media. The following topics may be included under this tenet:

- plagiarism
- hacking
- file sharing
- posting incorrect/inaccurate information
- stealing or pirating software, music and videos
- gaming
- copyright
- fair use
- online etiquette protocol
- cyber bullying
- online gambling
- internet addiction

# Be aware. Be cyber safe

# Cyber Bullying

## do not be a victim



SACSAA South African Cyber Security Academic Alliance

NRF

Microsoft

UNISA college of science, engineering and technology

www.cyberaware.org.za

# CYBER BULLYING

Bullying is no longer limited to the bus or playground environment; kids also use technology to intimidate and harass (to bully).

Cyber bullying can range from embarrassing or cruel online posts or digital pictures, to online threats, harassment and negative comments, to stalking through emails, web pages, text, and IM (instant messaging). While any age group is vulnerable, teenagers and young adults are common victims, and cyber bullying is a growing problem.

The same rules apply online as in the 'real world' about how to treat other people. Unfortunately, people don't always treat each other well online, and you or a friend may find that you are the target of cyber bullying. You may be teased or have rumours spread about you online, receive nasty messages or even threats. It can happen in school, or out of school hours, any hour of the day, and can come from people you know, and sometimes people you don't know. It can leave you feeling unsafe and alone.

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

Note the following if you are being cyberbullied:

**TIPS**

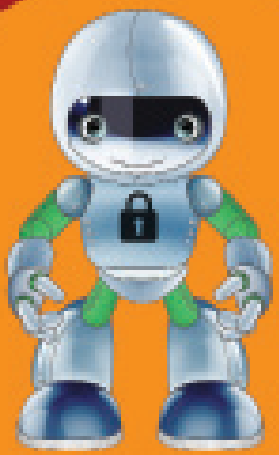
- **Ignore it.** Don't respond to the bully. If he/she doesn't get a response he/she may get bored and go away.
- **Block** the person. This will stop you seeing messages or texts from a particular person.
- **Tell someone.** Tell your mum or dad, or another adult you trust.
- **Keep the evidence.** This can be useful in tracking down the bully. Save texts, emails, online conversations or voicemails as proof.
- **Report the cyber bullying to the following:**
  - your school – it should have policies in place about bullying and cyber bullying
  - your ISP and/or phone provider or the website administrator – there are actions they can take to help
  - the police – if there is a threat to your safety the police will help

play

Be aware. Be cyber safe

# It's not only a game

## it's reality

NRF Microsoft UNISA

www.cyberaware.org.za

## What to do if a friend is being cyberbullied

- It can be hard to know if your friends are being cyberbullied. They might keep it to themselves. If they are being cyberbullied, 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 friends or lose interest in school and social activities.

## Help stop cyber bullying!

- **Stand up and speak out! I**f 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 often involves interaction with other computers and live players. It's fun for kids to connect with others, but it's important for them to avoid posting pictures of themselves or releasing other personal information to their fellow gamers. They should also know what to do if another player starts harassing them.

TIPS

### Gaming tips for parents

- Before your kids start playing, be sure your computer has an activated security suite: a firewall, anti-spyware software, and antivirus software.
- Be sure your kids have strong passwords for their gaming accounts. Passwords should be at least eight characters long and contain letters, numbers and symbols.
- Let your kids know they can come to you if they feel uncomfortable when playing a game.
- Participate in the game with your kids.
- Make sure your kids know how to block and/or report a cyber bully. Tell them to keep a record of the conversation if they are being harassed and encourage them not to engage the bully.

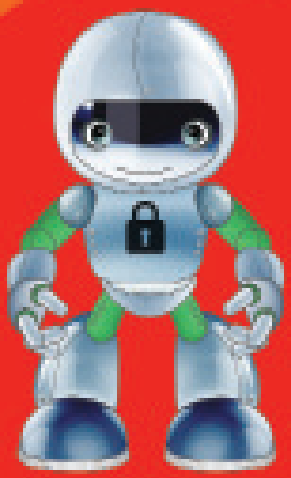

- Make sure your child's user name does not give away his/her real name, location, gender, age or any other personal information. (Examples of good user names are beach01, book2.)
- Make sure your kids use an avatar, and not an actual picture of themselves.
- If your kids are playing a game that features live voice chat, make sure they are disguising their voice. If the game does not have this feature, do not let them use voice chat.
- Limit the time that they are allowed to play games.
- Make sure you read and understand the ratings for the games that your children are playing. Some game sites have multiple games with different ratings, so check all of them.
- Keep the computer out in the open so that you can monitor your kids' online activities.
- Make sure your kids know that they may not send out any material to fellow gamers that contains private information and/or data.
- Use built-in parental controls on your Web browser.
- Don't let your children download anything without your permission. This includes cheat programs that may claim to help your child perform better in the game, but could really be carrying malware.
- Remember that prohibition won't work. Your children will use computers and games consoles, even if it's at school or at their friends' houses. If you talk to your kids about risks and good judgement, they will be able to get a lot more out of the web.

## Gaming tips for kids, tweens and teens


- Before you start playing, be sure your computer has an activated security suite: a firewall, anti-spyware software and antivirus software.
- Use a strong password for your gaming accounts. Be sure your password has at least eight characters and uses numbers, letters and symbols.
- If another player is making you feel uncomfortable, tell a trusted adult.
- Learn how to block and/or report other players if they are making you feel uncomfortable. Keep a record of what the other players said, but do not engage them.
- Never reveal your real name, location, gender, age, or any other personal information. Keep your user name vague.

Be aware. Be cyber safe

# protect yourself against Viruses

NRF Microsoft UNISA

www.cybersecure.org.za

- Use an avatar rather than an actual picture of yourself.
- Do not present yourself as dating material.
- Do not use voice chat when playing an online game, unless there is a feature that allows you to disguise your voice.
- Do not use a webcam while playing an online game.
- Place a time limit on yourself for game playing.
- Do not accept downloads from strangers. This includes cheat programs that may claim to help you perform better in the game, but that could in actual fact be carrying malware.
- Do not send out material to fellow gamers that contains personal information and/or data.
- Do not meet a stranger from your gaming world in person. People are not always who they say they are.
- Before you start playing, be sure your computer has an activated security suite: a firewall, anti-spyware software and antivirus software.
- Use a strong password for your gaming accounts. Be sure your password has at least eight characters and uses numbers, letters and symbols.

## ONLINE ETIQUETTE PROTOCOL

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.

**TIPS**

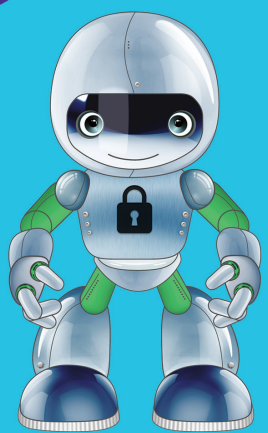
- **Treat other people the way you would like to be treated.** Avoid using bad language and don't say things to someone to make them feel bad.
- Learn about the **'netiquette'** of being online. What is considered okay to do and say and what is not? For example, if you type a message to someone in UPPER CASE letters they may think you are shouting at them.
- If someone says something rude or something that makes you feel uncomfortable, **don't respond**. Leave the chatroom or forum straight away.
- **Tell your parents** or another adult you trust if you read upsetting language, or see nasty pictures or something scary.

# Be aware. Be cyber safe

# Making friends online!

## Tips for safe social networking

- Be careful not to reveal personal information online.
- Only add people as friends if you know them in person.
- Delete inappropriate messages from your profile.
- Do not give information about your friends, it is unsafe.
- What you post online can be seen by everyone.



SACSAA South African Cyber Security Academic Alliance

NRF Microsoft UNISA college of science, engineering and technology

www.cyberaware.org.za

# Be aware. Be cyber safe

# Don't be blind for Cyber Crime



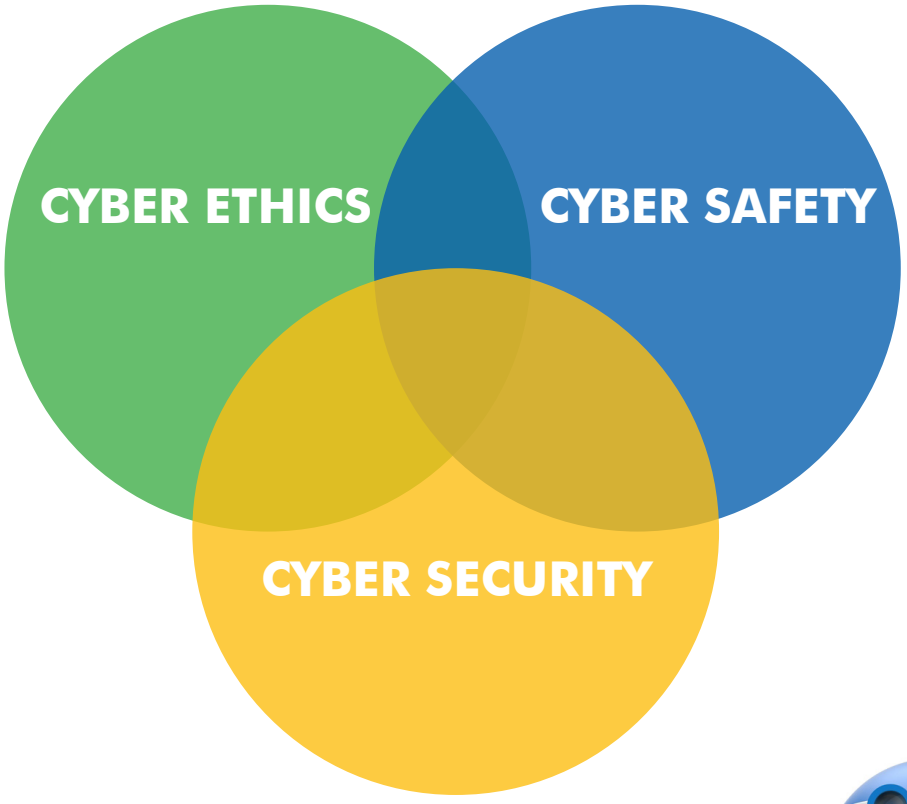
SACSAA
South African Cyber Security Academic Alliance

NRF

Microsoft

UNISA
college of science, engineering and technology

www.cyberaware.org.za




# CYBER SAFETY

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 behaviours can protect personal information and one's reputation, and include safe practices to minimise danger – from behavioural-based rather than hardware-/software-based problems. Topics that may be included under this tenet are as follows:

- online predators
- cyber stalking
- objectionable content
- pornography
- harassment
- hate groups
- unwanted communications
- online threats

## UNWANTED COMMUNICATIONS

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 who 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.

What should you do?

**TIPS**

- **Tell someone.** Tell your mum, dad, an older brother or sister, or another adult you trust.
- **Don't respond** to messages and leave the site or chat session immediately.
- **Block** the contact using your 'ignore' list or with filtering software.
- **Keep the evidence.** This can be useful in tracking the person posting unsuitable material or asking you questions.
- **Report it.** Ask your parents to contact your ISP and/or phone provider or the website administrator, as there are actions they can take to help. You can also report it to the police if there is a threat to your safety.
- **Set your profile to 'private'** so that your personal details are kept secret and it's harder for people you don't know to contact you.
- **Don't open messages** from people you don't know. These people could be nasty, their messages could contain viruses or they could be trying to sell you something.

## OBJECTIONABLE CONTENT

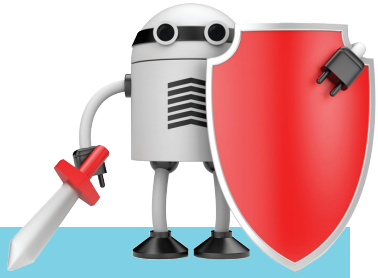
Online, children can be exposed to material that is inappropriate or even harmful to them. This could be material that is sexually explicit, offensive or violent. It may also be material that contains content that is racist and encourages hatred toward particular groups, or material that encourages unsafe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


Children and young people may not deliberately seek out inappropriate content. They may be inadvertently exposed to such content through otherwise innocuous activities such as:

- unexpected results from online searches

- clicking on unknown links within websites or emails
- incorrectly typing a web address or clicking on a pop-up ad
- clicking on online game content or prize offers

In some cases children and 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.



**TIPS**

- **Tell your parents** or another trusted adult if you come across material that upsets you.
- **Know how to 'escape'** from a website if an internet search takes you to an unpleasant or nasty website. Hit **'control-alt-delete'** if the site will not allow you to exit.
- If a website looks suspicious or has a warning page for people under 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 **instal 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.

## CYBER STALKING

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.

# Young children

Online stalkers or cyber stalkers use the internet or another form of electronic communication persistently to cause another person to feel apprehension or fear.

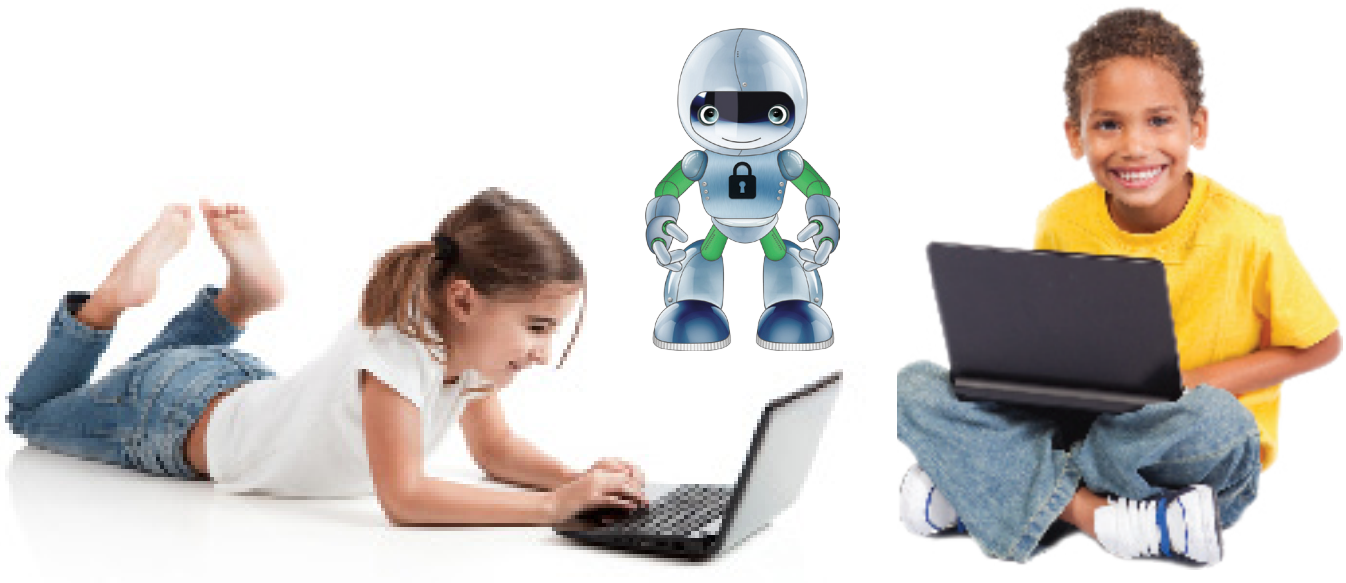
Online stalking is serious and should be referred to the police or independent legal advisors.

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. The following tips are useful to help children begin to manage online relationships.

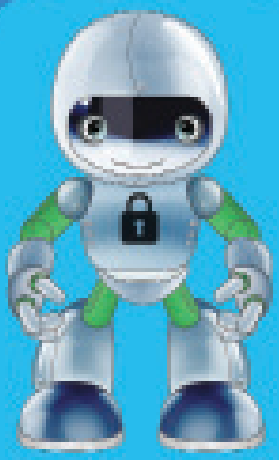
**TIPS**

- Teach children not to respond to or retaliate against any mean or unpleasant contact such as rude emails or messages.
- Teach them to tell a trusted adult when anything happens online that worries them, and help them to identify at least two trusted adults they can tell.
- Establish rules about the types of content or information they should report to an adult. For example, one rule may be: "Tell mum or dad about any swearing or bad words you find."
- Introduce the concept of personal information, which is information that can be used by others to identify their name, address, school or clubs.
- Make rules to restrict them providing personal information online. Young children will need simple rules such as: "You must check with mum or dad before you can type your address into the computer."
- Consider using filters, labels and safe zones to help manage your child's online access.
- If there is a threat to your child's safety, the police can help.



# Be aware. Be cyber safe

# Protect yourself against Cyber Predators



NRF Microsoft UNISA

www.cybersafe.org.za

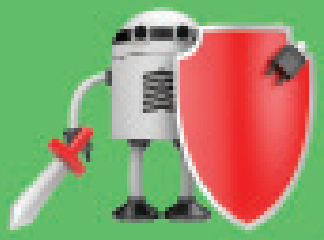
# Older children

Online stalkers or cyber stalkers use the internet or another form of electronic communication persistently to cause another person to feel apprehension or fear.

Older children may become more interested in websites and gaming sites that allow direct interaction with others including teens and adults. The following tips can help you manage the risk of cyber stalking for your child.

**TIPS**

- Explore your child's favourite websites. In general it is useful to consider whether you are comfortable with the content of the sites and the potential for contact with others, including teens and adults. Is your child socially ready to manage contact from potentially ill-meaning strangers?
- If you agree to your child accessing sites which may allow direct contact with others, consider establishing rules about the amount of information they can provide, including not providing their surname, address or name of school, and not uploading or SMSing images or videos without parental permission.
- Help children develop an avatar or false identity so that they aren't using their real name online.
- Teach your child not to respond or retaliate to any mean or unpleasant contact such as rude or intrusive emails or messages.
- Establish rules around the types of content or information they should report to an adult. For example, one rule may be: "Tell mum or dad about any swearing or bad words you find."
- Talk to your child about the use of location-based services. These services enable social networking users to report their physical location to other users by 'checking in'. Some services let people report their friends' locations and have location-based functions turned on by default. Your child can review their settings and block this function or limit who sees their location-based information. Remind your child that allowing strangers to see where they are, or where their mates are, is risky behaviour.
- Consider using filters, labels and safe zones to help manage your child's online access.
- If your child shows changes in behaviour or moods that are concerning, including changes in friendship groups, anxiety, sadness, clinginess or withdrawal, explore your concerns with him/her and if necessary seek professional support.



# Be aware. Be cyber safe

# Protect your identity



www.cyberaware.org.za

MCSAA NRF Microsoft UNISA

Be aware. Be cyber safe

# Firewalls
## protect your computer



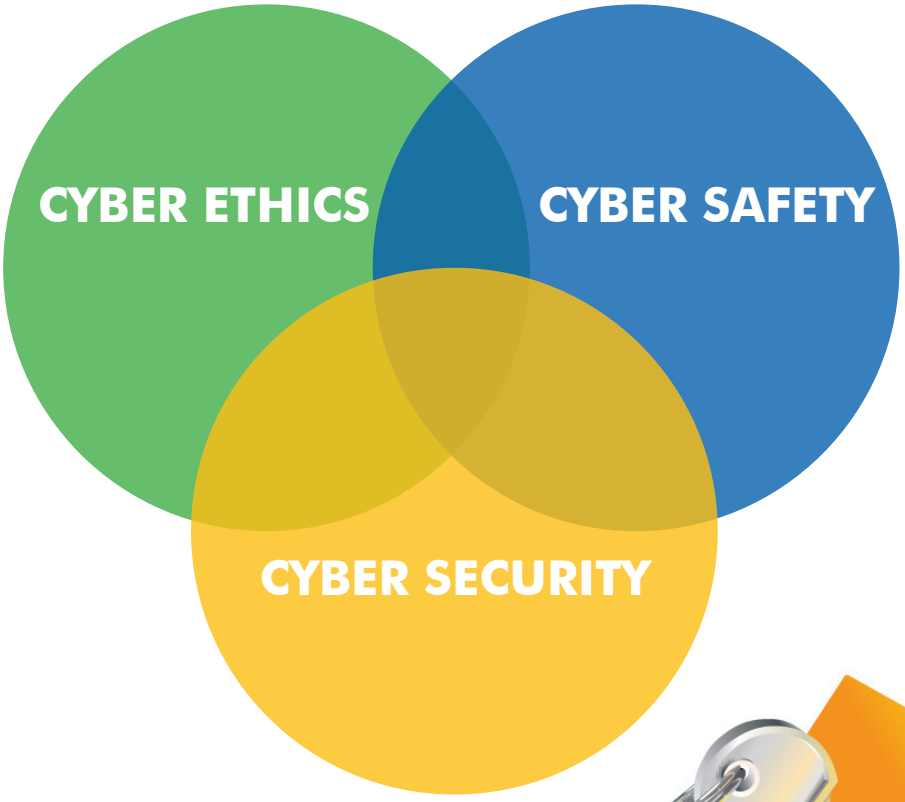
SACSAA
South African Cyber Security Academic Alliance

NRF

Microsoft

UNISA
college of science, engineering and technology

www.cyberaware.org.za




# CYBER SECURITY

Cyber security is defined as "the vulnerability of any computing system, software program, or critical infrastructure to, or their ability to resist, intentional interference, compromise, or incapacitation through the misuse of, or by unauthorized means of, the Internet, public or private telecommunications systems, or other similar conduct that violates Federal, State, or international law, that harms interstate commerce of the US, or that threatens public health or safety". Cyber security is defined to cover physical protection (both hardware and software) of personal information and technology resources from unauthorised 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. Topics that might be included under this tenet are as follows:

- theft of identity
- phishing
- hoaxes
- ponzi schemes
- spoofing
- pharming scams
- chain letters
- criminal scams
- spyware
- privacy

| | |
|---|---|
| • hacktivists<br>• viruses<br>• get-rich-quick schemes<br>• junk email | • adware<br>• trojans<br>• malware |

## THEFT OF IDENTITY

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 criminalssing 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.

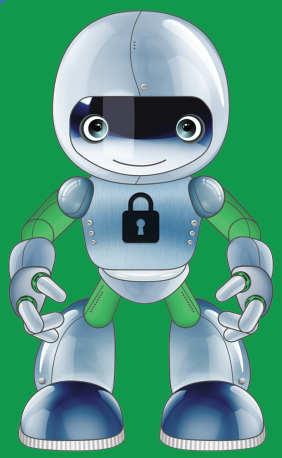
Criminals use many methods to gather personal information, including sending viruses and spam, and setting up fake websites. You can also have your identity 'stolen' if someone uses your personal information to impersonate you online. They might pretend to be you, make a fake profile of you or hack into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

**TIPS**

- **Watch your blog/profile.** If your profile has been hacked, shut it down as soon as possible.
- **Use secure websites** for online shopping and banking. Make sure the website is secure. More secure website addresses start with 'https' rather than the less secure 'http'. Alternatively, a padlock image should appear in the browser.
- **Protect passwords.** Passwords should be eight or more characters in length. Change them regularly and don't write them down or store them where they are openly available. Never share your passwords, even with your friends – these could be misused to access your MSN, email or profile.
- **It's not just your passwords.** Don't post personally identifiable information online. Each little bit of information can be put together by identity thieves to build a total picture and steal your identity. Set profiles to private and don't blog or tweet personal information.
- **Watch your bank account.** Respond immediately to any unexpected withdrawals or spending. Look out for small amounts of money being withdrawn

# Be aware. Be cyber safe

# Phishing
# is an illegal way to obtain your personal information



SACSAA

NRF

Microsoft

UNISA college of science, engineering and technology

www.cyberaware.org.za

TIPS

unexpectedly. This may be a criminal testing your account details prior to withdrawing a larger amount.

- **Don't get phished.** Don't respond to calls or emails from any bank asking for passwords or other details. Banks never send emails asking you to click through to their site – if the email asks you to click on a link, chances are it's a scam. If you receive a call from someone saying they're from the bank, hang up and call back at the publicly listed number to see if it's real.

## Phishing

Scams are ways of obtaining information or money through false means. Spam is an unsolicited commercial electronic message. Phishing is the use of email or SMS to encourage individuals to reveal financial details like credit card numbers, account names and passwords or other personal information. Phishing messages can look like genuine messages from a real bank, telecommunications provider, online retailer or credit card company.

The following tips will help with the management of scams, spam and phishing:

TIPS

- Avoid giving out your email 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?
- Warn children and young people about accepting unknown friends or causes on social networking sites – unknown contacts or causes have been linked to identity theft scams.
- Do not respond to unknown SMSs asking you or your children to make contact and provide cash or financial information. If a phone or email contact seems unusual, especially if money is involved, hang up or do not reply.
- If you are concerned that you or your child may have been the target of a scam, contact your local consumer affairs agency. If your child has provided a suspected scammer with financial information, contact the local police and your financial institution directly.
- Remember that banking institutions will never contact customers by email seeking specific account details. Contact your bank directly using verified contact details if you have any concerns about a contact from a source claiming to be your bank.

- Only disclose financial information on websites that you trust and that have secure payment facilities identified by a web address beginning with https:// and a 'locked' padlock symbol in the bottom of the screen, which indicates that data is being encrypted.
- If a website you usually use for purchases or banking looks unusual or behaves differently, contact the organisation directly using a known phone number or one obtained from a trusted source.
- If you receive an email that seems suspicious, for example you don't recognise the sender or the subject line looks dubious, delete it and don't click on any links within it.
- 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 organisation, you can unsubscribe through an email link or SMS 'STOP'.
- Instal and update antivirus and other e-security software to restrict unauthorised 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.

## Viruses


Viruses infect computers when infected files are downloaded onto a vulnerable computer. These vandals wantonly 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.

The following tips can help you implement and maintain adequate e-security measures.

**TIPS**

- **Use strong passwords.** Use long and random passwords for any application that provides access to your personal information, including logging into your computer.
- Ideally, the password should be eight or more characters in length, not a dictionary word, contain a mixture of letters and numbers and contain a mixture of upper and lower case letters. Change passwords regularly and use different passwords for each application.
- **Instal and update antivirus and other security software.** Viruses and other malicious software, such as worms and trojan horse viruses, can alter or

erase data on your computer and allow spammers and other intruders to use your computer and network.

- Viruses and worms spread fast, and new variations are constantly being released, so antivirus software must be updated regularly.
- **Antivirus software** should be set to automatically scan all incoming and outgoing emails and any devices that are intermittently connected to a computer, such as a memory stick, a music player, digital camera or other USB device. 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 defence against intruders. Firewalls can block all traffic between your network and the internet that is not explicitly allowed, preventing unauthorised access to your data. A firewall should be used in conjunction with antivirus and anti-spyware software.
- **Manage emails safely.** Delete suspect emails immediately. If you do open an email that seems suspect, don't click on any links in the email. All email 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 emails and report spam to the ACMA.

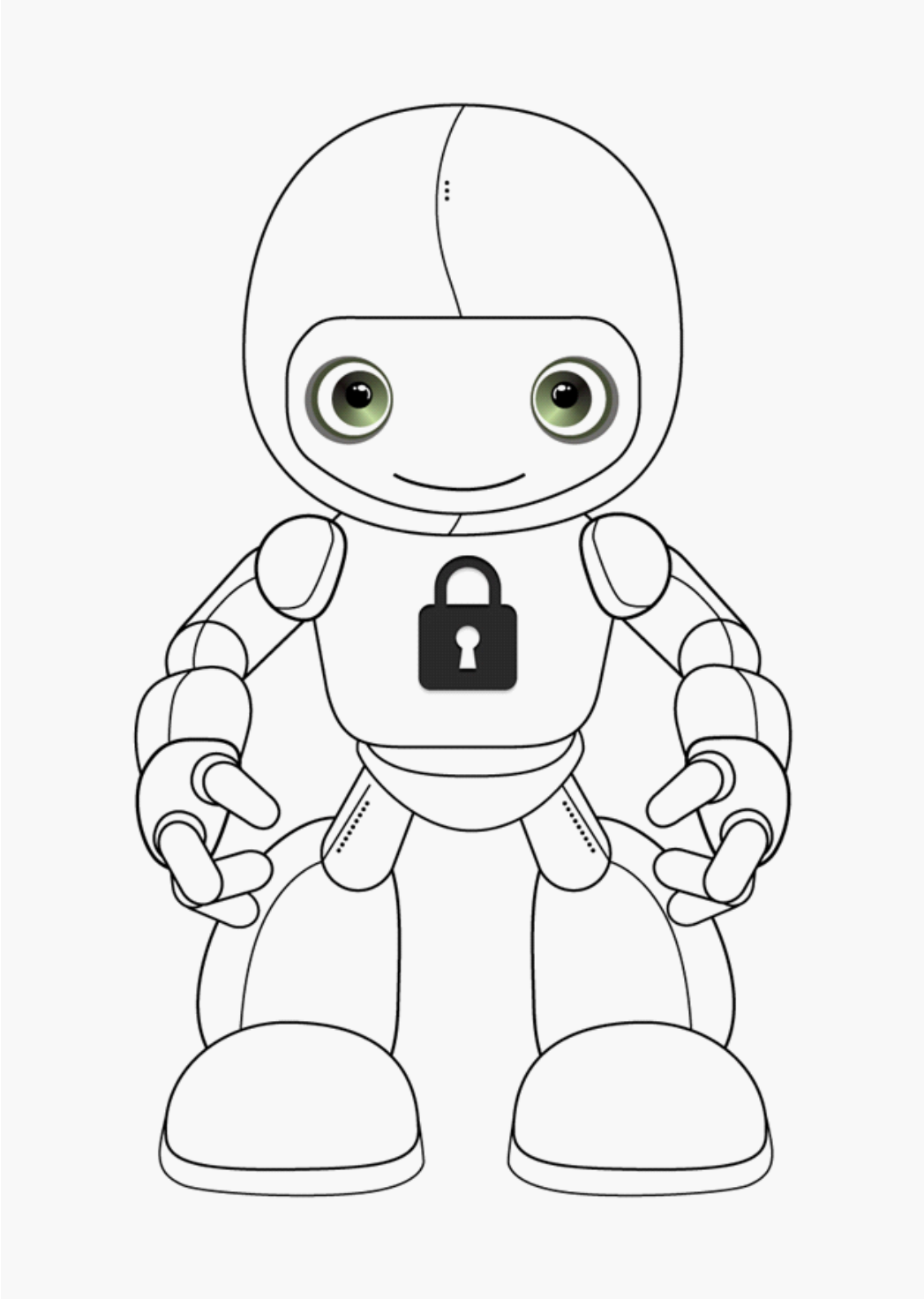

- **Use safe internet browser settings.** When browsing the web, creating documents, reading email and playing games, using a limited permission account can prevent malicious code from being installed onto your computer. A 'limited permission' account is an account that does not have 'Administrator' 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 instal these patches when necessary.
- **Check and alter default settings.** After installing software, check the configuration and setting options – you may find the software has extra features you don't need or want. Turning off unnecessary services is a good security precaution.
- **Back up your data and files.** Back up your data regularly and check that backups are working. Creating a copy or backup of data is an effective way to help recover information from a computer if a virus destroys files, or the computer is stolen or destroyed. For example, burn data, photos, videos etc on to a CD-Rom or a USB stick, or use an external hard drive regularly.
- **Use caution when sharing or downloading files.** Don't download files or

applications from suspect websites. The file or application could be malware. Sometimes the malware may even be falsely represented as e-security software designed to protect you.

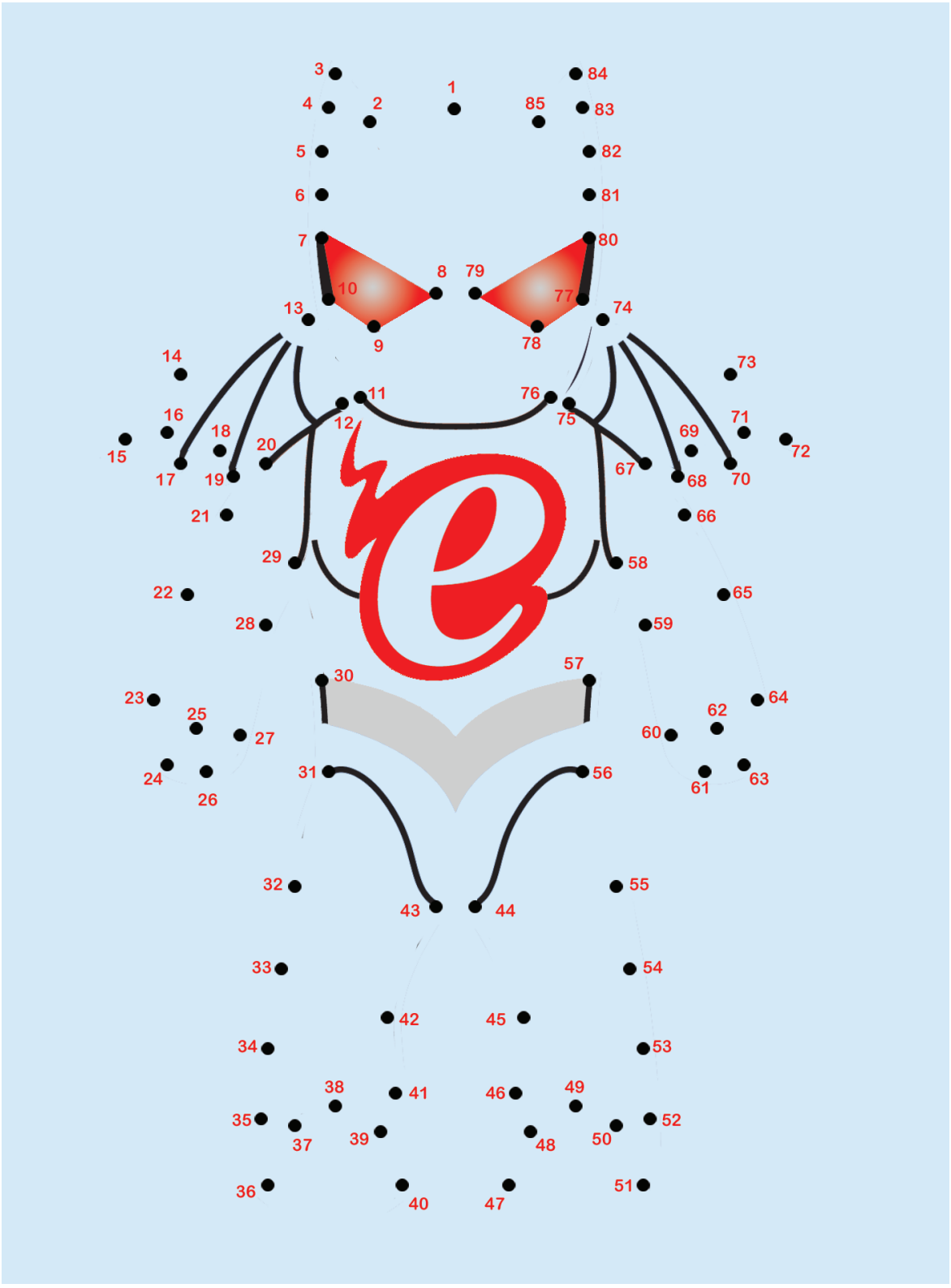
- **Protecting wireless internet connections.** Wireless networks require special attention to secure them from hijacking.
- Users should change the default password to a strong password or turn off the SSID broadcast on the wireless router to engage the highest level of encryption available for their wireless network, including turning the WPA encryption on restrict access to the wireless network with MAC address filtering. To monitor wireless networks for unusual activity turn off the wireless connection when not in use.
- Internet service providers or software vendors will be able to provide specific advice about protecting wireless networks.
- Keep up-to-date with security information. Users can keep up-to-date with security advice that affects their systems.


# ACTIVITIES

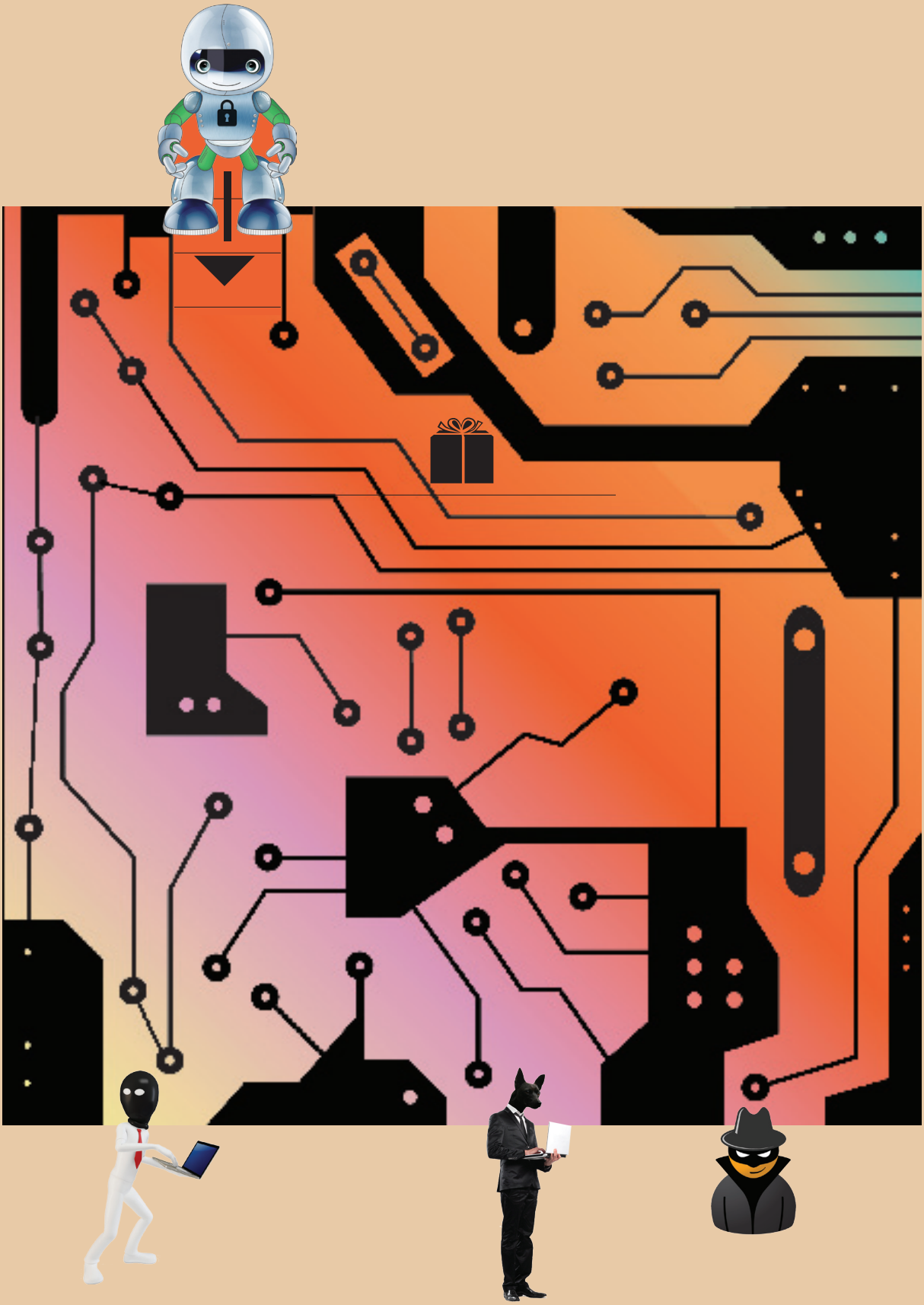
## Colouring in



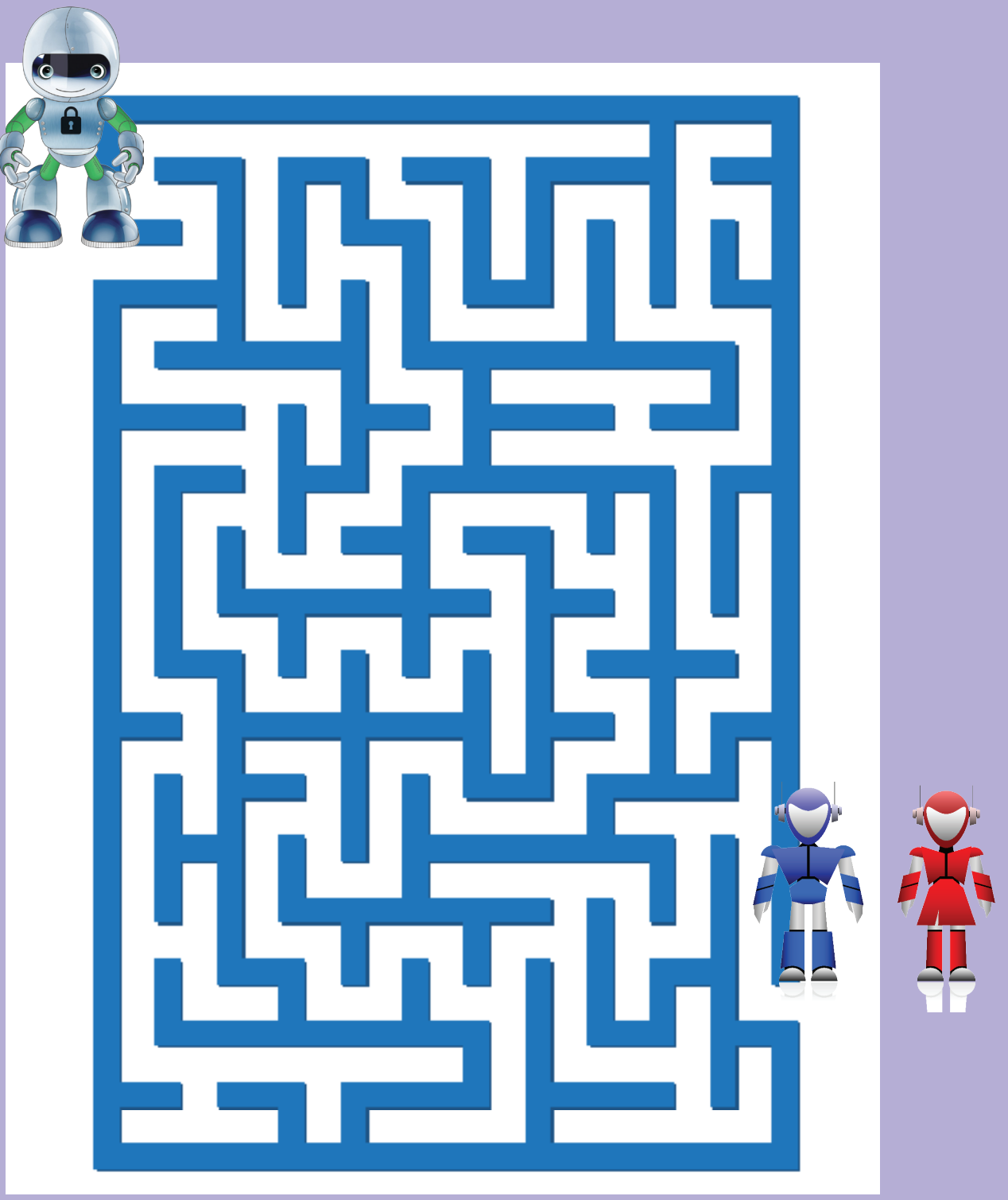
# Connect the DOTS



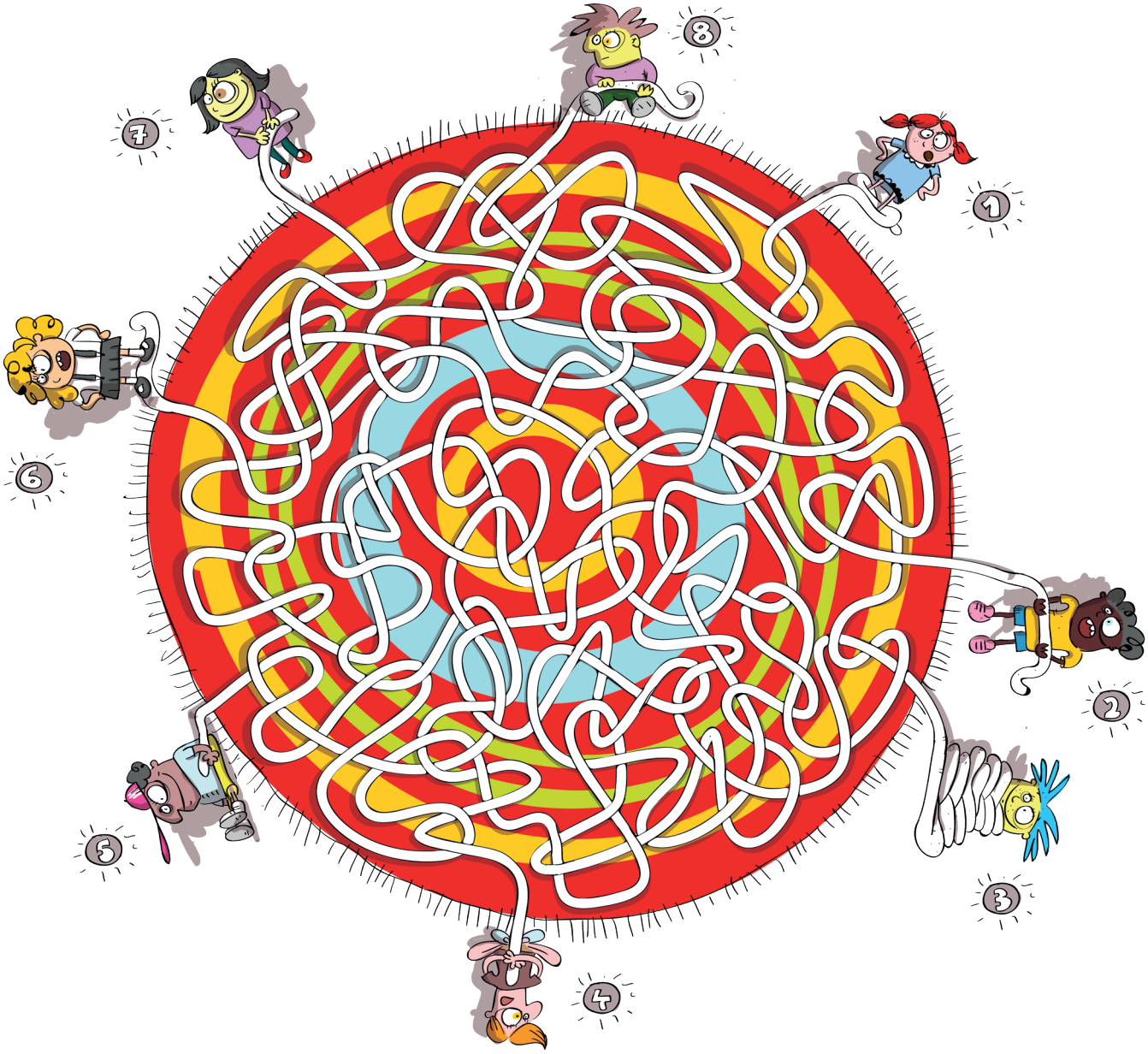
# Help Cyber Safe Robot to catch the criminals



## Help Cyber Safe Robot to find his friends



**Each of these people has a friend. Connect them with eachother**



## Draw lines to connect the correct terms with each other

| | |
|---|---|
| Virus | Online harassment |
| Treat people online in the same way you would like to be treated | Facebook |
| Cyber bullying | Phishing |
| Social networking | Netiquette |
| Email | Malicious user of computing systems |
| Identity theft | Personal information used without your permission |
| Hacker | Malicious code |

## Uncramble the letters to reveal the correct cyber awareness-related term

RVISU

YEDITNIT TTFHE

RBCYE LULIBNYG

RPTCOGIYH

QNEUETTTEI

BRECY TSAKLIGN

GPINSHIH

WPAYRES

OJRSTAN

# Cut out the square.

Fold paper from corner to corner to make a triangle.

Fold the triangle from corner to corner again, making a smaller triangle.

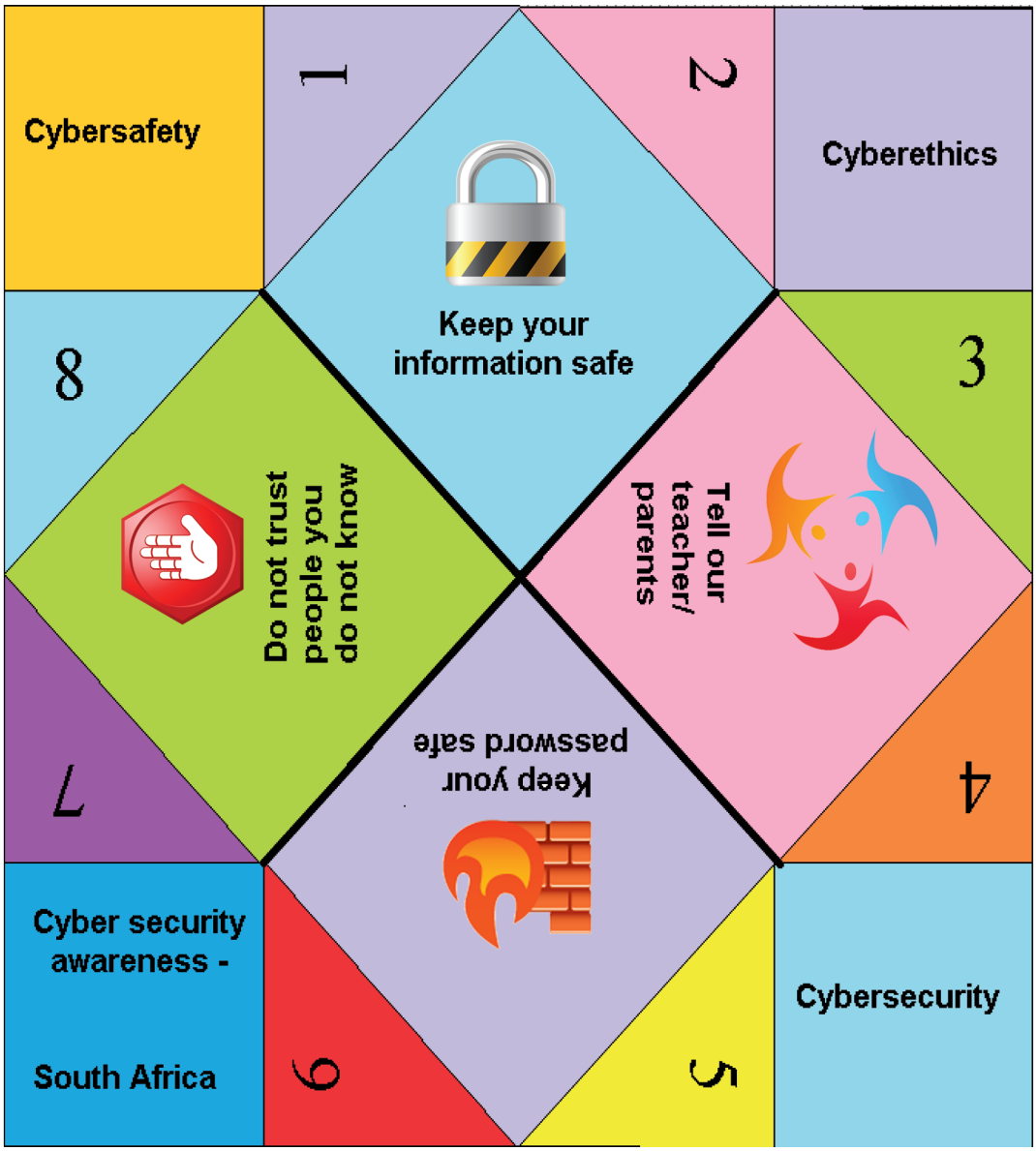
Unfold.

Fold the four corners to the centre of the square.

Turn the paper around.

Fold four corners to the centre of the square.

Push the four corners of the square into the centre and then slide four (4) fingers into the flaps of your fortune teller.



## Draw lines to connect the correct terms with each other

| | |
|---|---|
| Virus | Online harassment |
| Treat people online in the same way you would like to be treated | Facebook |
| Cyber bullying | Phishing |
| Social networking | Netiquette |
| Email | Malicious user of computing systems |
| Identity theft | Personal information used without your permission |
| Hacker | Malicious code |

## Uncramble the letters to reveal the correct cyber awareness-related term

RVISU

YEDITNIT TTFHE

RBCYE LULIBNYG

RPTCOGIYH

QNEUETTTEI

BRECY TSAKLIGN

GPINSHIH

WPAYRES

OJRSTAN

AMIGPAIRSL

# Search for and circle the cyber awareness terms

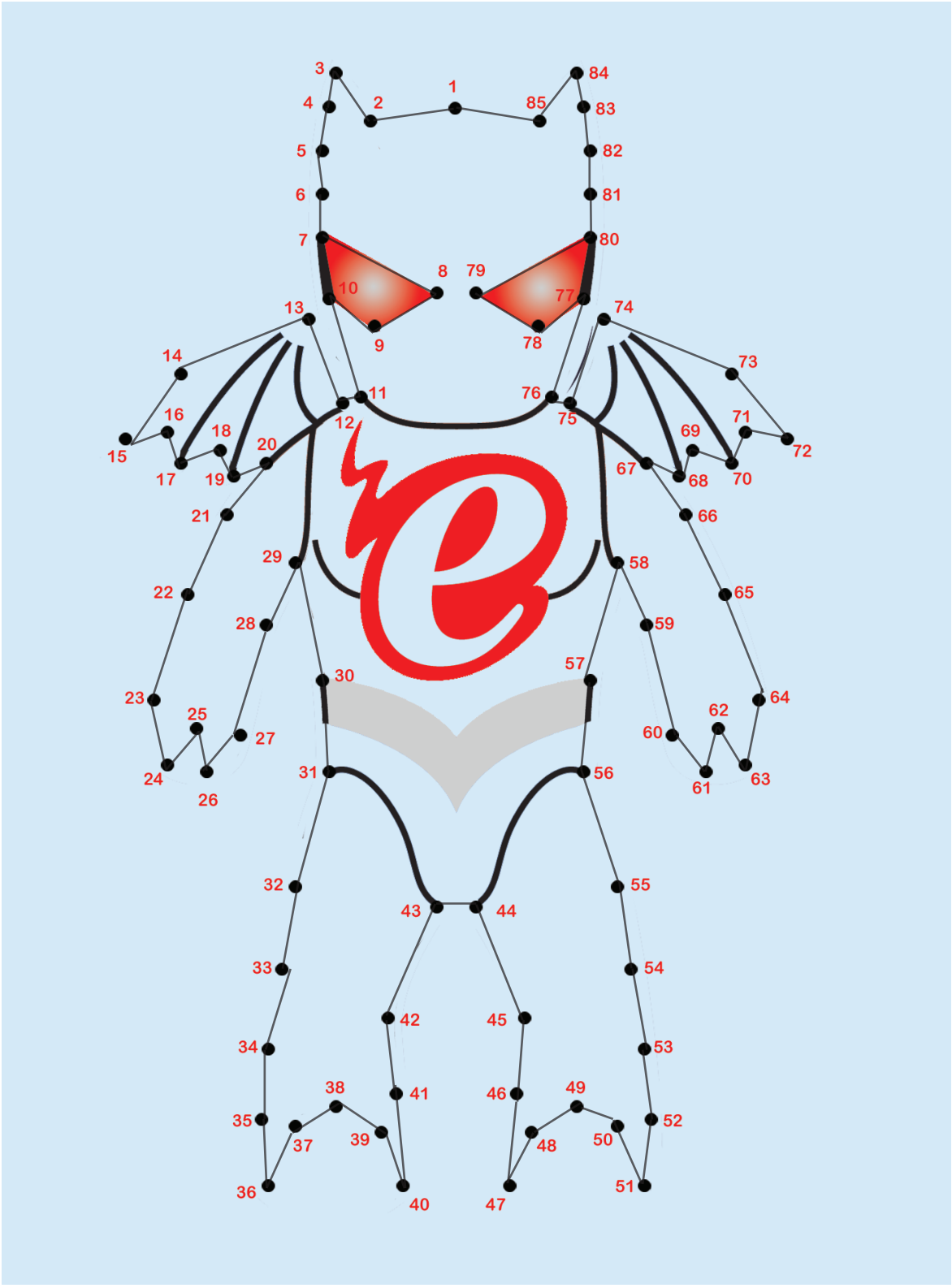
Look for the following cyber awareness terms in the block below and circle them. The words can be in any direction (from left to right, from top to bottom, from bottom to top or diagonal):

CYBER STALKING
HACKING
CYBER ETHICS
VIRUS
HARASSMENT
COPYRIGHT
CYBER SECURITY
SPOOFING
PLAGIARISM,
CYBER SAFETY,
PHISHING
SPYWARE

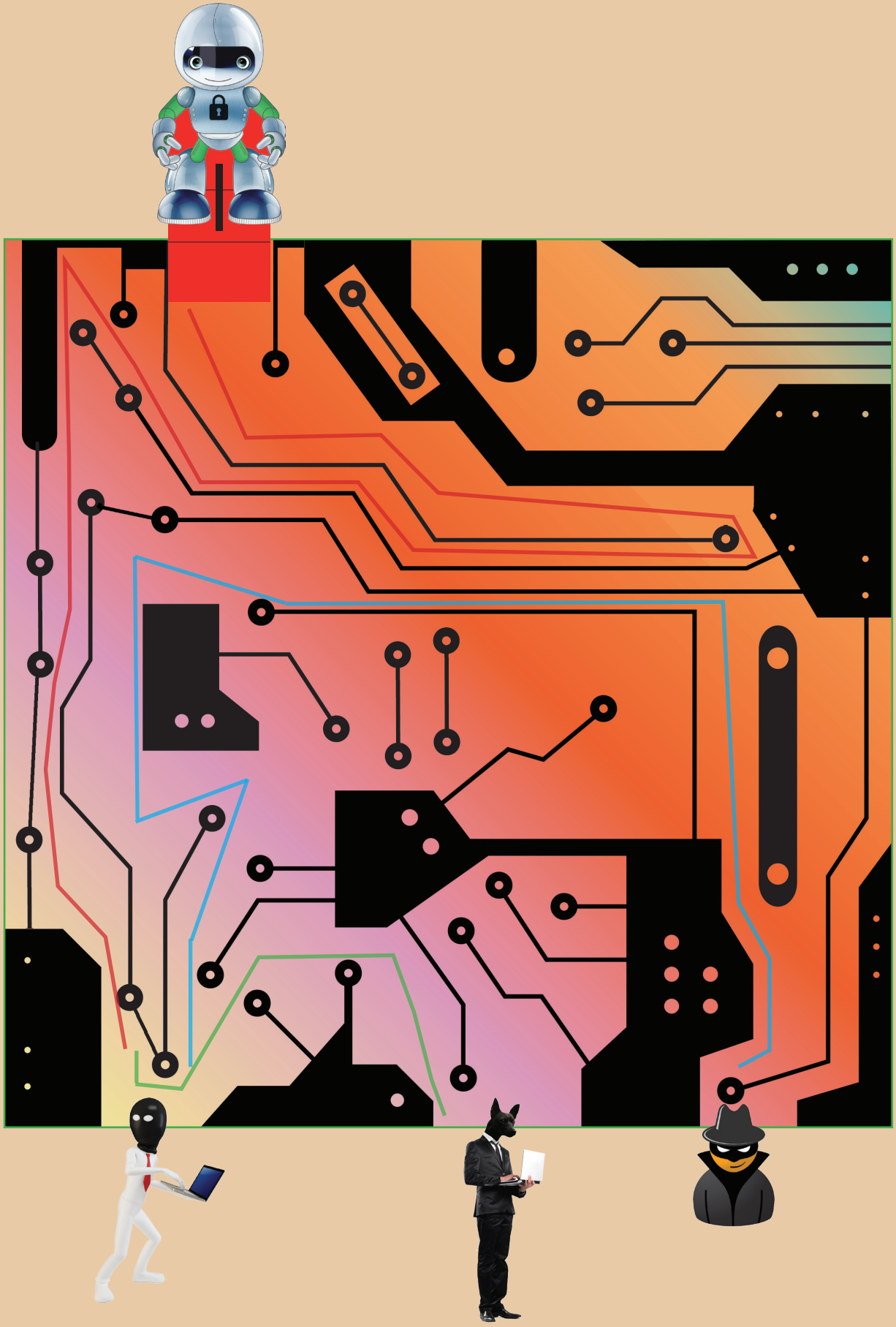
| C | Y | B | E | R | S | E | C | U | R | I | T | Y | P | G | L |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | T | B | D | U | L |  | C | R | W | T | Z | A | H | H | K |
| Q | H | P | I | G | S | S | Y | F | E | Y | F | S | I | F | J |
| S | G | O | S | D | U | P | B | V |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

# ANSWERS

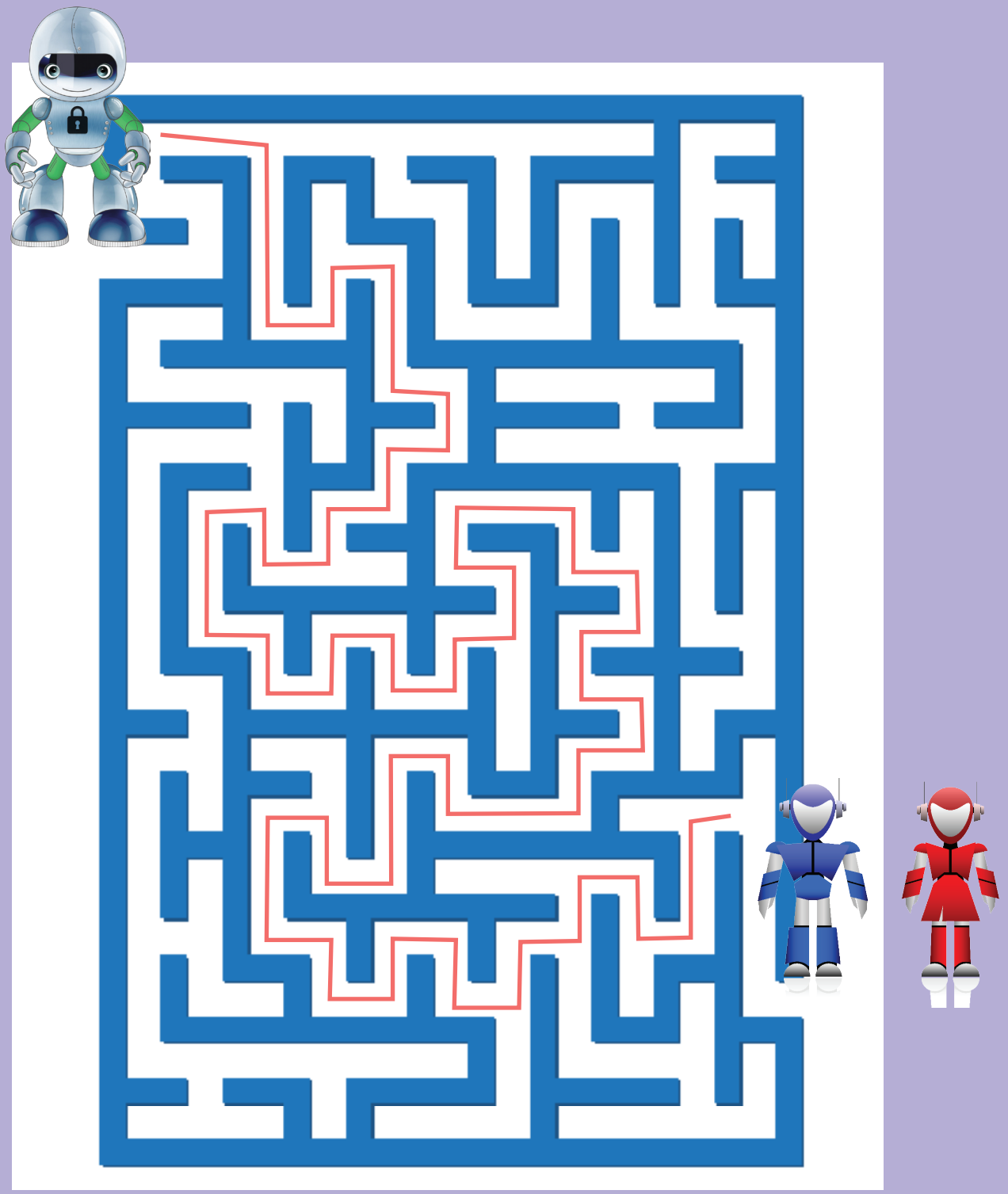
## Connect the DOTS

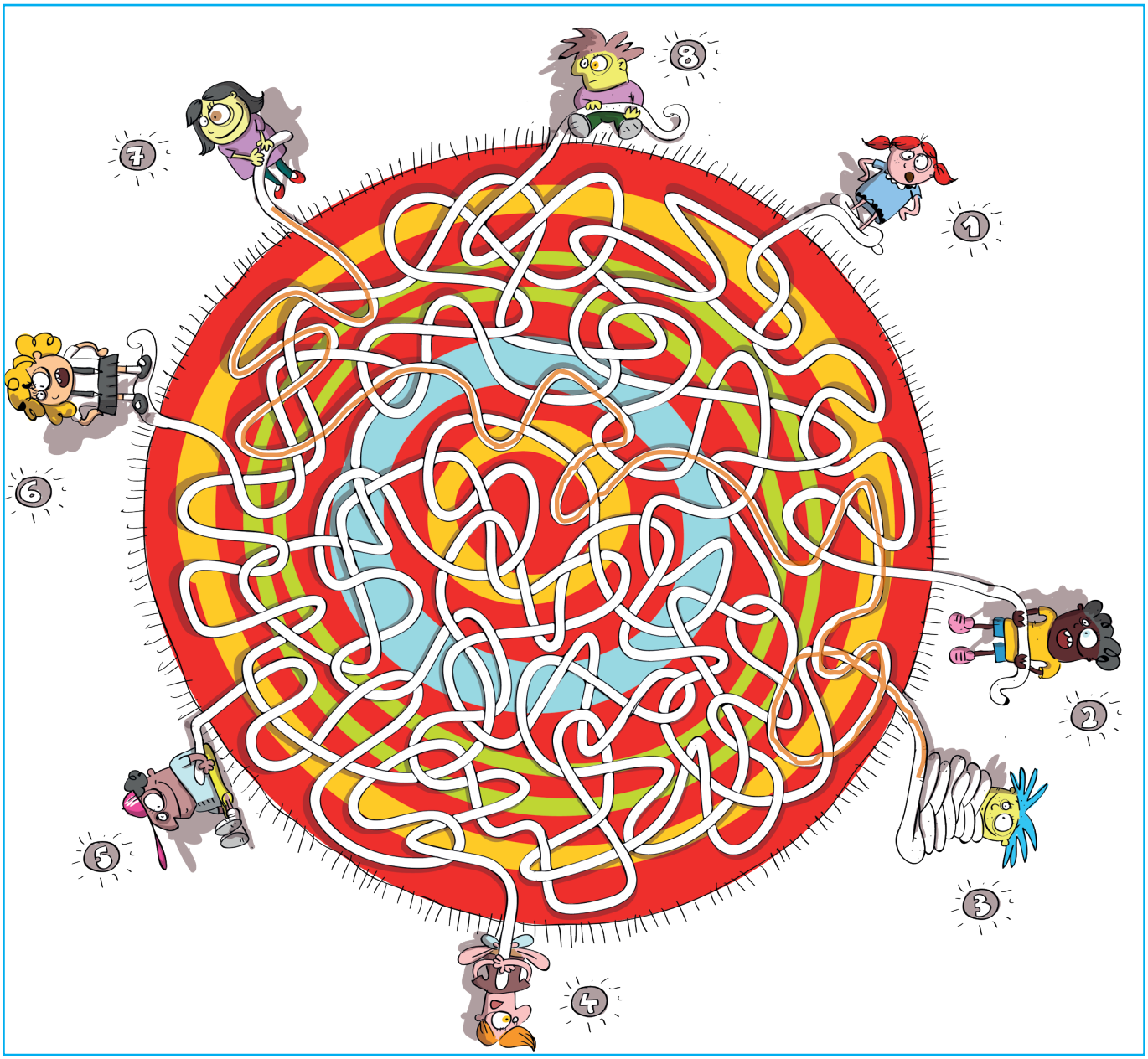


# Help Cyber Safe Robot to catch the criminals



## Help Cyber Safe Robot to find his friends




1
2
3
4
5
6
7
8

## Draw lines to connect the correct terms with each other

| | |
|---|---|
| Virus | Online harassment |
| Treat people online in the same way you would like to be treated | Facebook |
| Cyber bullying | Phishing |
| Social networking | Netiquette |
| Email | Malicious user of computing systems |
| Identity theft | Personal information used without your permission |
| Hacker | Malicious code |

## Uncramble the letters to reveal the correct cyber awareness-related term

VIRUS

IDENTITY THEFT

CYBER BULLYING

COPYRIGHT

NETIQUETTE

CYBER STALKING

PHISING

SPYWARE

TRIJANS

PLAGIARISM

# 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 |

# REFERENCES


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

© 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.

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

Reservation of rights:

All Contents (including, without limitation, the graphics, icons, and overall appearance of the website 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 website and the contents are intended only for the individual, non-commercial use of website users. No user of this website may resell, republish, print, download, copy, retransmit or display (by use of an html "frame" or otherwise) any portion of this website 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.safetyweb.com/poster

SafetyWeb is excited to provide the online safety community with a Free Poster illustrating some alarming statistics about cyber bullying. We encourage everyone to download and utilize this free resource to help educate your community about online safety!

http://www.cyber.edu.in/index.php?title=Posters

Asian School of Cyber Laws has prepared posters for spreading awareness on various aspects of cyber safety.

These posters can be freely downloaded in high-resolution PDF format for easy printing.

http://www.nativeintelligence.com

Free Security Awareness Posters

Terms of use: Copyrights must stay with the free posters; the posters must not be changed, and the images must not be extracted.

http://www.protect.iu.edu/cybersecurity/downloads

The Information Security and Policy Offices generate and provide educational materials regarding computer use and security. Feel free to download these and use them, either printed or electronically, in your campaign. Generally, work on these sites may not be used for commercial purposes. The only exception is for educational purposes on awareness campaigns, providing that the campaign is internal to the organization in scope and materials received from this site will not be used or seen publicly.

http://www.iu.edu/comments/copyright.shtml

The Indiana University website includes a variety of materials created by different members of the IU community. Although these works may be freely accessible on the World Wide Web and may not include any statement about copyright, the U.S. Copyright Act nevertheless provides that such works are protected by copyright. Users must assume that works are protected by copyright until they learn otherwise.

Indiana University would like users to make productive use of materials found on this Web page, particularly if the uses are for non-profit educational purposes. The university is currently seeking means to clarify the rights of use of many materials accessible on its Web pages. Unless rights of use are clearly stated with respect to an individual item, users must seek permission from the copyright owner for all uses that are not allowed by fair use or other provisions of the U.S. Copyright Act. If you need assistance with identifying or locating the copyright owner of a work, please contact the owner of the page from which you linked to this statement. If you believe there has been an infringement of your copyright, you can make a complaint to IU's Chief Privacy Officer and Compliance Coordinator.

https://cyberexchange.isc2.org/download.aspx

I'm Security-Conscious, 2! Help the people in your community and your organization adopt this mantra by downloading any of these fun, free security awareness tools posted on the (ISC)$^2$ Cyber Exchange. We encourage you to share these materials with anyone in your community or workplace that would benefit - whether it's your friends, colleagues, or children. You can also rank your favorites. Help us make the cyber world a safer place!