Get Cyber Safe Agency

Workbook for kids
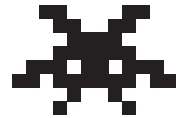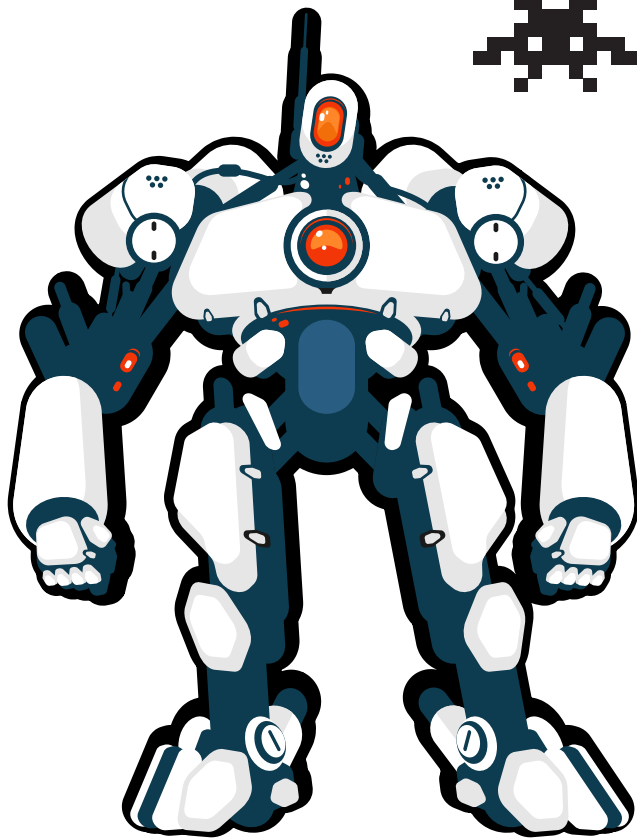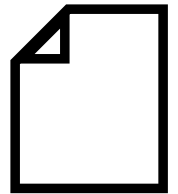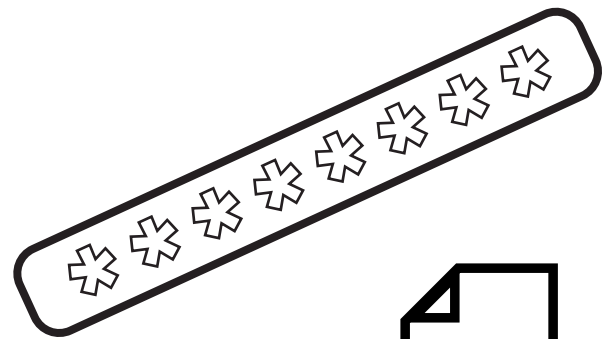
Communications Security Establishment   Centre de la sécurité des télécommunications

GETCYBERSAFE.CA

Canada
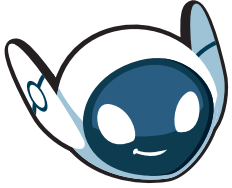
Welcome to your first mission!

Hi Cyber Agent! I'm your partner, Cybot. Together, we're going to take down the cyber villain, Viro. Viro attacks innocent people online and steals from them. We need to stop them!

Ready to get started? Great! The first step to defeating Viro is to set you up with a **passphrase**.

Let's see how much you know about passwords and **passphrases**. Let's do some Cyber Agent training and take the quiz below to find out.

Before you start your mission: If you ever come across a new word that you aren't familiar with, you can look up the definition in the **glossary** on page **21** of this workbook! Good luck, Cyber Agent!

Cyber Agent training: Passphrases

Instructions:

Answer the following questions by circling the right answer! You can find the correct answers to all quiz questions at the back of the booklet.

Question 1: When is it OK to share a password?

A   Never

B   Only with your besties

C   Whenever someone needs it

Hint: Passwords protect **all** the information on your account!
Hint: Passwords are **very** personal!

Question 2: True or false: It's safe to use the same password more than once.

A   True

B   False

Hint: If a cyber criminal steals your password, they can access **all** your accounts that use that same password.

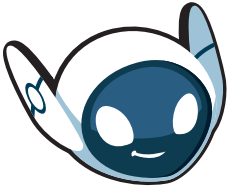### Question 3: What type of password is the strongest?

A   A passphrase made of four or more random words

B   A password that's as short as possible

C   A password with your pet's name in it

Hint: Passwords should never include information about you.
Hint: Longer passwords are stronger passwords!
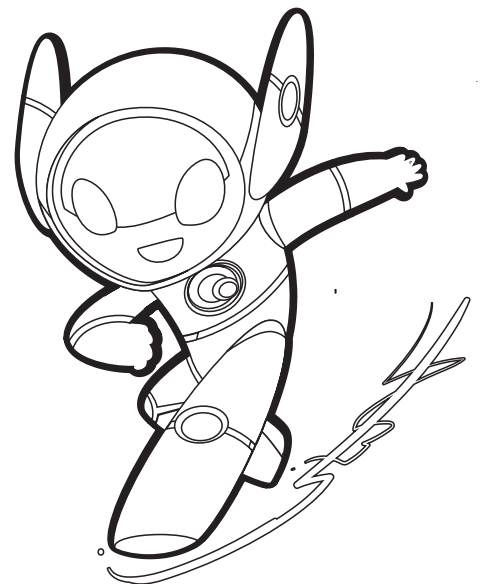
Great job, Cyber Agent!

Before we can start our mission, we'll need to create a strong top-secret passphrase to protect our secret cyber agent files and accounts from Viro (and other cyber criminals). Now that you know about passwords and passphrases, let's create one together!

How to play

→ Write an answer to **four** of the questions below

→ Try to use **one-word answers** that have **at least four letters**

→ In the last box, write all your answers down together to get your top-secret passphrase!

→ You can use your passphrase results for one of your accounts or devices (remember, we want to use a unique passphrase for each account)!

Answer four questions below to create a top-secret passphrase!

What is your least favourite vegetable? _____

If you had $100, what would you spend it on? _____

Name something blue you can see right now. _____

What did you eat for lunch yesterday? _____

What day of the week is it? _____

Choose a random word that starts with L. _____

Name an object in your kitchen. _____

Your top-secret passphrase is:

Great work, Agent!

Now that you're set up with a top-secret passphrase, let's start your next mission.

Great job creating a super top-secret password by using a passphrase!

Now comes even more fun... spy tools! We're going to pick out the tools you need to fight Viro.

Before you start grabbing tools, let's go over what we need to defeat Viro. First, we'll need an **anti-virus software** to help keep away bad files called **malware**. We should also grab a **hard drive** or make sure you have space in your cloud storage. Then you can make backup copies of important files.

And don't forget to grab extra protection called multi-factor authentication or MFA, using things like a fingerprint or personal identification number or PIN.

We've got a lot of spy tools to take with us. Let's do some more Cyber Agent training to figure out just what we need.

Cyber Agent training: Tools

Instructions:

Answer the following questions by circling the right answer! You can find the correct answers to all quiz questions at the back of the booklet.

Question 1: How do you back up a file?

A Save the same file two times on the same device

B Save a copy of the file in a safe place that's not on the same device

C Delete the file

Hint: Backups keep your files safe if something bad happens to your device.
Hint: It's best to keep backups somewhere secure.

Question 2: What is multi-factor authentication (MFA)?

A An extra way to prove that you are who you say you are (like a PIN code or fingerprint)

B A long word

C A riddle to trick cyber criminals

Hint: Multi-factor authentication (MFA) is used when you log in, like in some of your video games.
Hint: "Authentication" means "proving that something is true".

Question 3: When should you update software?

A Whenever I can

B When my phone is super slow

C When the pop-up reminder message won't go away

Hint: Software updates keep your devices safe!
Hint: It's better to update your software **before** something goes wrong!
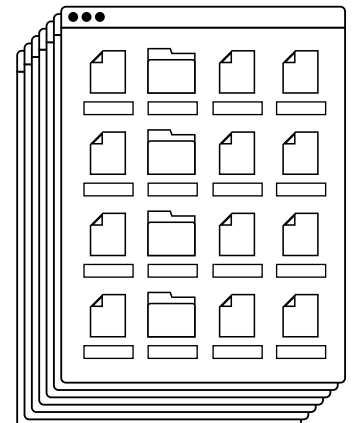
Excellent work, Agent!

Now that you know how to protect your tools, we can pack our spy kit for the mission ahead! Let's figure out what we need to pack, together.

How to play

Pack your spy kit for the mission ahead by colouring each item that you think we need to defeat Viro. Don't colour the items we don't need. You can check your work after by flipping to the next page!
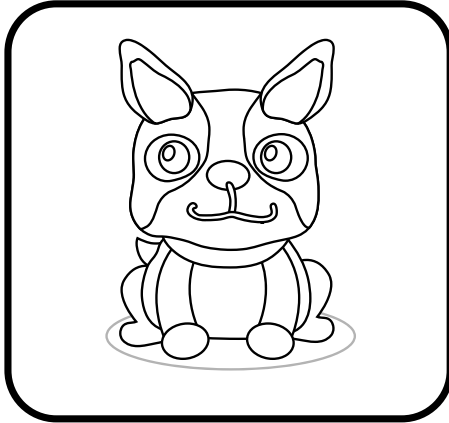
Puppy
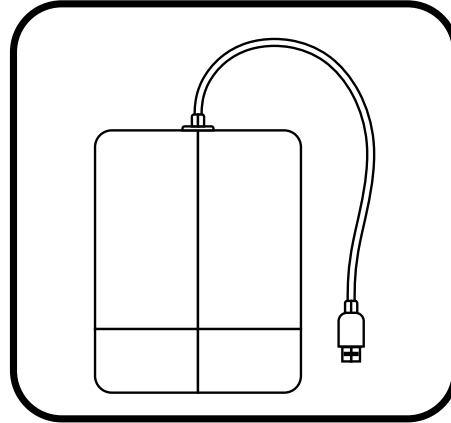
Hard drive

Firewall
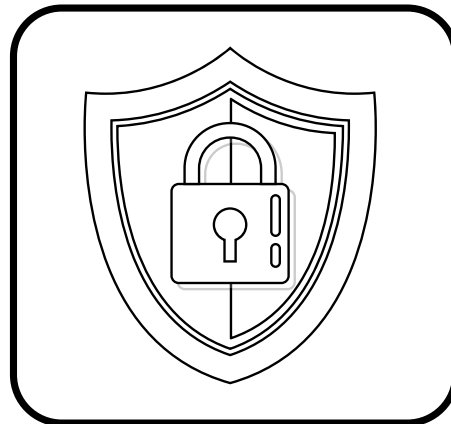
Anti-virus software
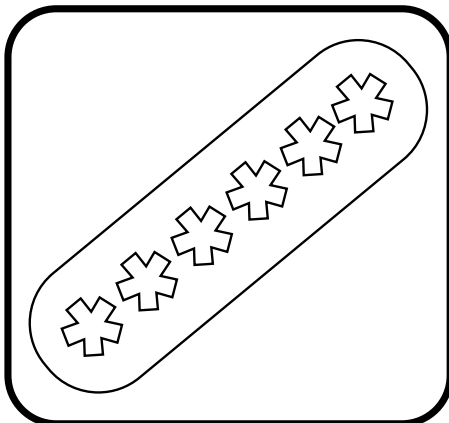
Passphrase
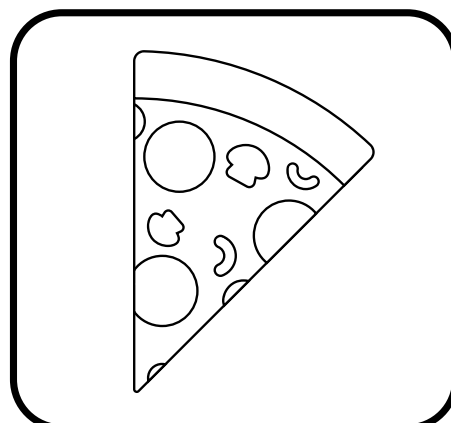
Pizza

Tools of the trade game answers:

Anti-virus software: Correct, you will need this!
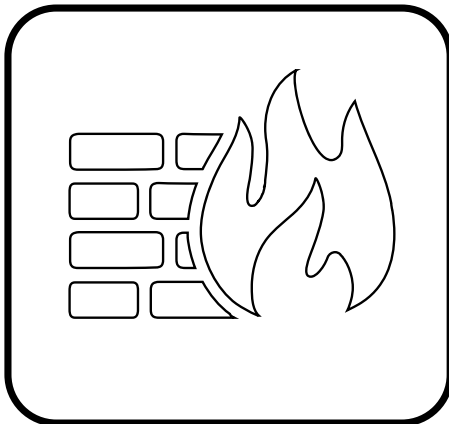
Anti-virus software will stop bad files and viruses from infecting our tools!
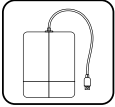
Hard drive: Correct, you will need this!

A hard drive is perfect for backing up all our important files, so we never lose them!

Puppy: Oops, you won't need this!

Puppies are fun and adorable sidekicks, but they aren't very good at getting cyber safe.
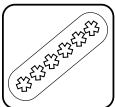
Passphrase: Correct, you will need this!

Passphrases are like passwords, but they're longer and safer!

Firewall: Correct, you will need this!

Firewalls do a great job at protecting our devices when they're connected to the internet!

Pizza: Oops, you won't need this!

Pizza sure tastes great, but it won't help to defeat Viro.
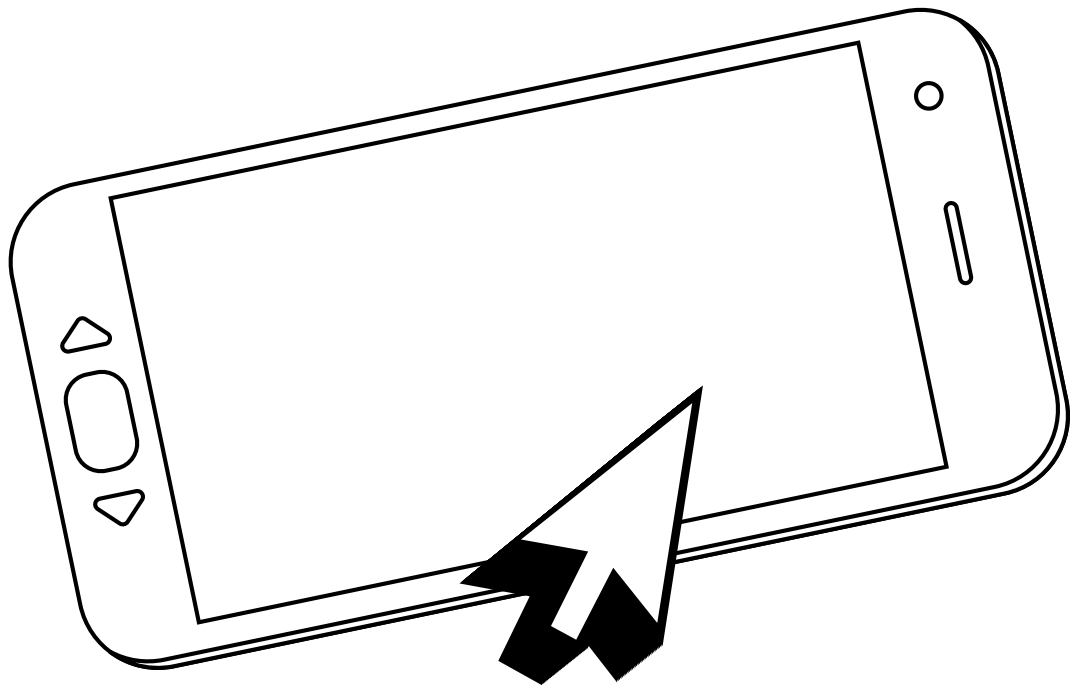
Fantastic work!

Now that you have your tools, you need to secure them from Viro. Can you help me set up our **Wi-Fi router**? It's a small device that connects our other devices, like tablets and phones, to the internet. Let's go through a checklist to make sure our router is secure.

First, let's make sure the router is somewhere away from the windows. Then, we'll give the router a secure password, just like you did earlier by using a passphrase! Later, you can ask an adult at home for help with your router.

Ready to get started? Let's put our minds together to secure our router.

Cyber Agent training: Wi-Fi router

Instructions:

Answer the following questions by circling the right answer! You can find the correct answers to all quiz questions at the back of the booklet.

Question 1: True or false: Updating your devices can help keep your Wi-Fi network safe.

A   True

B   False

Hint: Updating your devices can help them stay protected.

Question 2: In your home, the safest place to put your router is:

A   In front of your front door

B   In the middle of your home

C   Hidden with your toys

Hint: A **router** is a small device that connects your other devices, like tablets and phones, to the internet.
Hint: The closer your devices are to your router, the stronger and faster your Wi-Fi is!
Hint: Cyber criminals can hack your Wi-Fi more easily if it's closer to them, like when it's near the outside of your house.

Question 3: When you set up your Wi-Fi for the first time, it will have its own password – a default password. Why should you change it to something new?

A   Cyber criminals can easily steal your Wi-Fi if you don't change it

B   A lot of other people may have the same built-in password

C   Both **A** and **B**

Hint: You should never keep a password that was given to you!
Hint: You can use a **password manager** to remember passwords or passphrases that are long.
Hint: Cyber criminals are really good at cracking passwords.
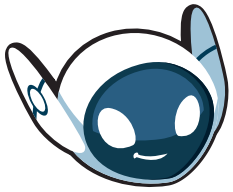
Excellent work, Agent! Now that you know how to protect a Wi-Fi network, let's do our best to make our network safe from Viro!

We just got news that Viro is planning a cyber attack against us. Let's work together to secure our Wi-Fi network before he does!

How to play

→ In the picture below, there are three empty circles where you can place a router. Draw a picture of a router in the most secure location in the house. You can also draw a picture of your router at home (you can ask a trusted adult if you aren't sure where it is) or draw a picture of just a router, like the one in the corner of this page.

→ Flip the page over after you're done to see if you got it right!
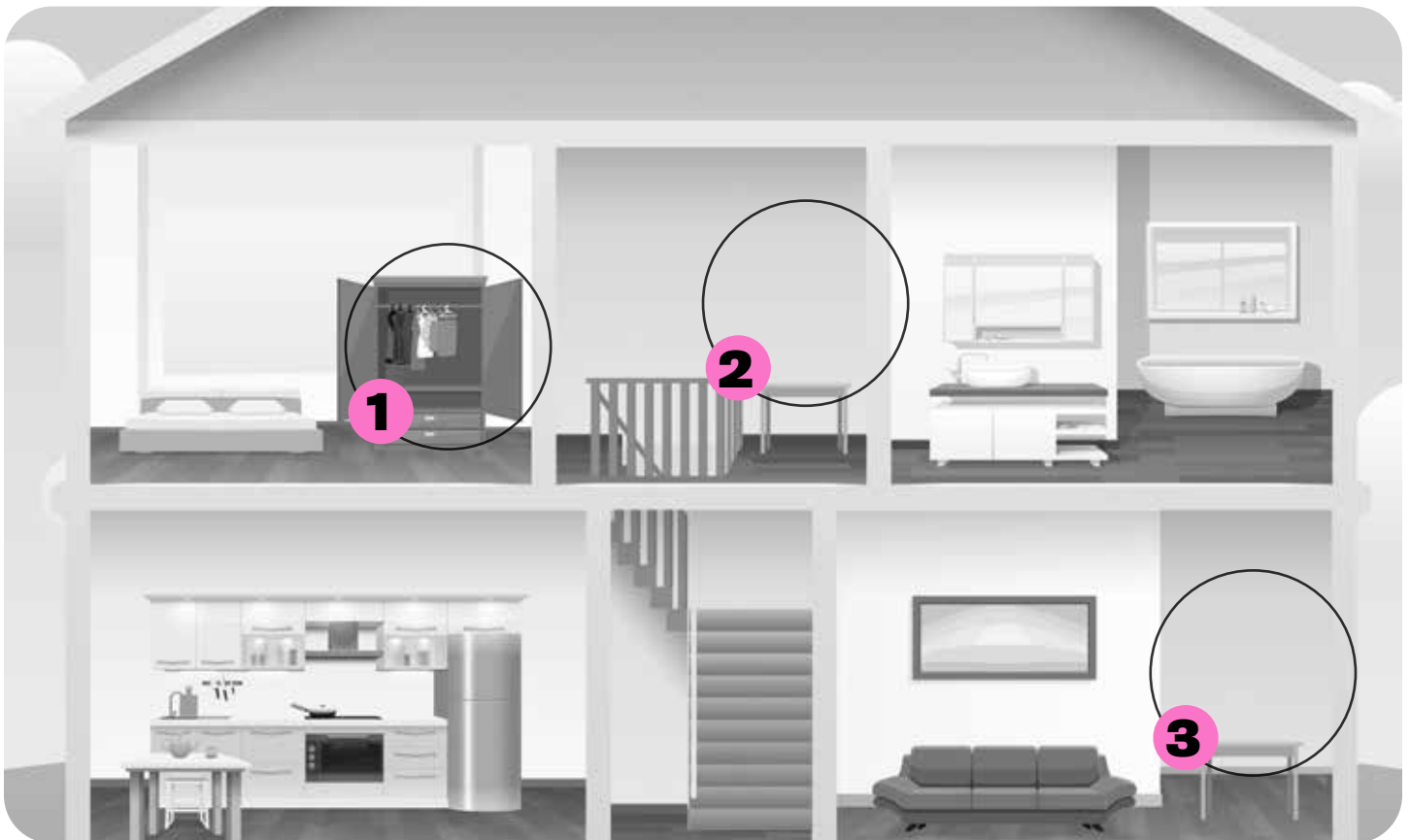
Location 1: In a coat closet

Location 2: In the middle of the home

Location 3: In front of a window
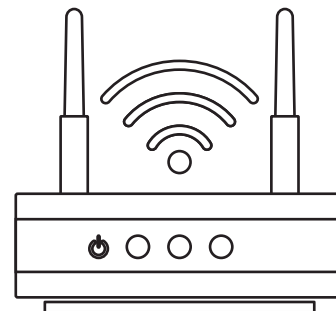
Answers:

Location 1 (in a coat closet): Oops! If your router is hidden somewhere, like a closet, it can make it difficult for you and your family to connect to your Wi-Fi!

Location 2 (in the middle of the home): Correct! Leaving your router somewhere in the middle of your home makes it easier for you and your family to connect to it, and more difficult for cyber criminals to access it!

Location 3 (in front of a window): Oops! The closer you are to your router, the stronger the Wi-Fi signal is. Leaving the router in front of a window could make it easier for strangers or cyber criminals to connect to it!
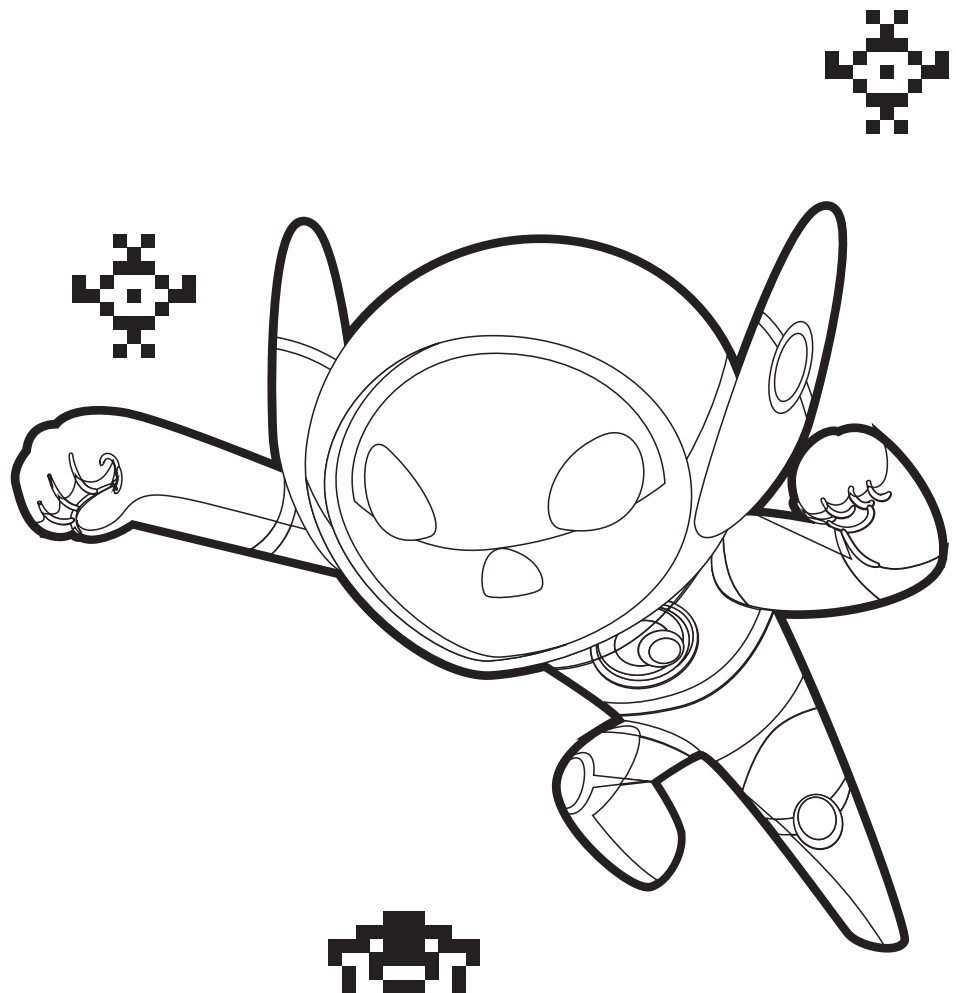
A clue just came in. Maybe we can use it to catch Viro!

Oh no! It looks like Viro's cyber criminals have also been sending us phishing messages to try and confuse us. Phishing messages are messages that cyber criminals send to pretend to be someone they're not. But some cyber criminals aren't good at being sneaky. Sometimes they'll make mistakes that you can spot, like using blurry images or using a silly email address. We can get to the bottom of this!

Let's sort through these clues by finding out which one is real and which ones are phishing messages.

Cyber Agent training: Phishing

Instructions:

Answer the following questions by circling the right answer! You can find the correct answers to all quiz questions at the back of the booklet.

Question 1: If you receive a message from a stranger asking you to download something, what should you do?

A   Ask a trusted adult for help and then delete the message

B   Open it. What's the worst that can happen?

C   Send the email to someone else

Hint: Messages from people that you don't know can be very dangerous!

Question 2: True or false: Not everyone online is who they say they are.

A   True

B   False

Hint: You shouldn't automatically trust people that you meet online.

Question 3: What are some clues that you can use to spot a phishing message?

A   Spelling mistakes

B   A silly looking email address

C   Strange links and attachments

D   All of the above

Hint: Sometimes cyber criminals make mistakes that let us know a message could be fake. Never click on anything that looks or sounds weird.
Hint: Cyber criminals may ask you for personal information, like your address or password. No one should ask you for any type of information about yourself in a message or voice chat.

Game 4: Phishing for Clues

Amazing work, Agent! Now that you know how to spot a phishing message, let's work together to sort through the clues that we just received.

Important clues about Viro's evil plans just arrived. It looks like some of the clues got mixed up with phishing messages that Viro sent to confuse us.

Let's work together to figure out which clues are real, and which ones are phishing messages.

How to play

→ Carefully read through each of the phishing messages. Circle the ones that you think are phishing messages so you know which ones to throw out later.

→ You can use the **Red Flags of Phishing** below to help you figure out which messages are phishing messages and which ones are real clues.

→ Flip to the back of the book after you're done to see if you found all the phishing messages!

The Red Flags of Phishing

Phishing flag #1:

A message rushing you to do something quickly

Example: "Click on this link right now before it's too late!"

Phishing flag #2:

A message asking you for personal information

Example: "Please click this link and send us your password to verify your account."

Phishing flag #3:

A message saying you won money, a prize or a contest

Example: "Congrats on winning a free vacation to Hawaii! Please send us $50 to claim your tickets."

Phishing flag #4:

A message filled with spelling mistakes in the email address, the message or in links

Example:

From: Uwhber231mKn56@mailbox.com

Message: Helo, im messging you for a amazone gift card, pleez respond soon! Clik

here: aamazone.com

Phishing flag #5:

A message from an unknown address that has weird attachments (like files, pictures, or folders)

Example: "Please download the attached file DefinitelyNotAVirus.bat"

Phishing flag #6:

A message filled with blurry images or a strange looking design

A

To: Agent@GetCyberSafeAgents.com

From: AwesomeAlex@Friends.com

Subject: Cyber Tip Hotline

Hi Agents,

I heard that Viro was planning a major cyber attack using malware. No more info at this time. Hope this helps.

B

To: Agent@GetCyberSafeAgents.com

From: NotViro@EvilPlans.com

Subject: A totally real clue!!1!

Heeeey, Agentz. I know wher u can find VIRO!!

Just click the link below! Rite now!! And u can find out too!!

[>>**CLICK HERE**<<]

C

To: Agent@GetCyberSafeAgents.com

From: Attack@EvilPlans.com

Subject: !FREE vacation!

Congratz agent!!!

You won a PRIZE! An all-expenses paid trip to Fiji! Don't worry about Viro! Just go on your trip!

Click the link below and send just $5 to claim your tickets!!!! Hurry! The offer ends soon!!

 [>>>**Click Here**<<<]

D

To: Agent@GetCyberSafeAgents.com

From: Vile@GetCyberCafeAgentz.ca

Subject: Need help!!!

Hi Agents!!

I am a new Cyber Agent. I lost my password and I need to borrow someone else's. Can Someone please reply to this email and send me their password so I can use it until I find mine? Thanks!!

Answers:

A Correct!

This message is safe. The sender isn't asking for strange information or asking us to click on anything. Let's keep this clue.

B Oops!

This message has a lot of typos and a suspicious link. Use the **Red Flags of Phishing** to help you figure out which messages are phishing scams!

C Oops!

It looks like whoever wrote this message wants to distract us with a fake prize. Use the **Red Flags of Phishing** to help you figure out which messages are phishing scams!

D Oops!

Whoever wrote this message is making an odd request. Use the **Red Flags of Phishing** to help you figure out which messages are phishing scams!
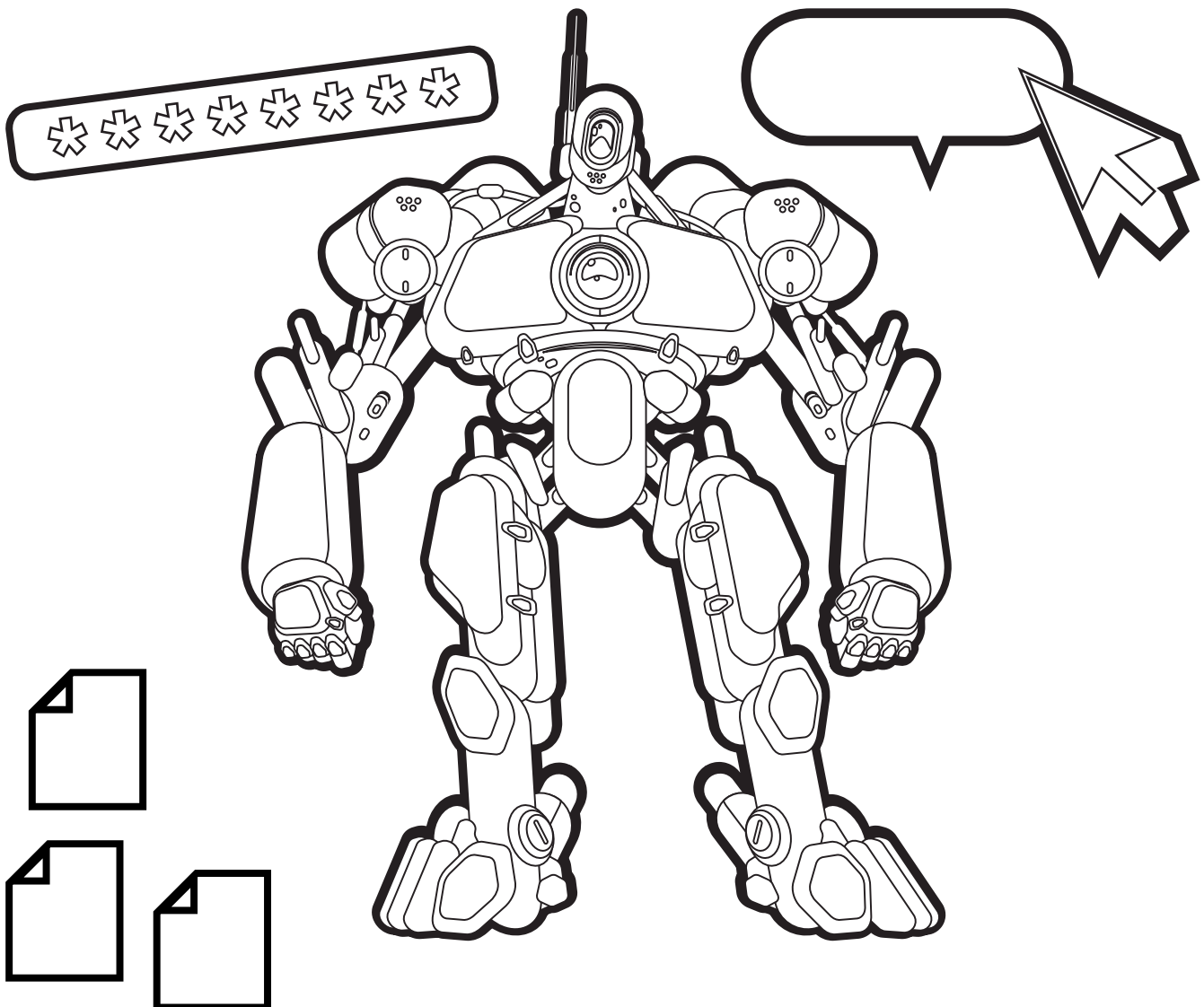
Uh oh! It looks like I accidentally clicked on a link in a phishing email, and now I can't access any of my files. Viro must have given me malware! As my partner, it's up to you to get rid of the malware. Once the malware is gone, you can access the files you need to defeat Viro.

There's a secret code that you can solve to crack the case. First, let's learn a little bit more about malware so we know how to get rid of it.

Cyber Agent training: Malware

Instructions:

Answer the following questions by circling the right answer! You can find the correct answers to all quiz questions at the back of the booklet.

Question 1: True or false: If you have backed up your data, you'll be able to get your stuff back if you ever accidentally download ransomware!

A   True

B   False

Hint: "Ransomware" is a bad file, made by cyber criminals, that you can download online. It will lock you out of your device, and the cyber criminal may ask you to pay them money to give it back.
Hint: "Backing up your data" means making a safe copy of all your device's information! This could include movies, games, pictures, and other important stuff.

Question 2: Malware is bad software that cyber criminals create to mess with your:

A   Data

B   Devices

C   Networks

D   All of the above

Hint: Malware is short for malicious software. You can usually get it from downloading something or clicking on a bad link.

Question 3: When is it safe to download stuff online?

A   When I get an email or text asking me to download something

B   If an adult I trust says it's OK or if it's from somewhere I've downloaded something safely before

C   Whenever I see something cool online

Hint: Some things are safe to download, but not everything is!
Hint: A download could really be a virus. Sometimes is hard to tell. It's better to be safe than sorry!

Game 5: Malware Bytes Back

Great work, Agent! Now that you understand a little more about malware, let's work together to solve the secret code that can help us get Cybot's files back.

How to play

→ Solve the secret code by matching the numbers in the empty spaces below to the letters that each number is assigned to.

→ When all the letters are solved, you'll receive a top-secret message that will tell you how to get Cybot's files back from Viro!

→ Once you've solved the top-secret message, flip to the next page to see what happens next!

| 5 | 14 | 1 | 4 | | 16 | 9 | | 6 | 12 | 16 | 3 |

| 17 | 11 | 15 | 2 | 8 | | 14 | 18 | 10 | | 10 | 2 | 7 | 11 | 1 | 2 | 8 |

A = 14	F = 17	N = 18	U = 16
B = 5	G =13	O =12	V = 7
C = 1	I = 11	P = 9	Y = 6
D = 10	K = 4	R = 3	
E = 2	L = 15	S = 8	

Top Secret Code:

Back up your files and devices

Congratulations, Cyber Agent!

Wow, you cracked the code! Great job, Agent! It looks like the secret message is to **"back up your files and devices."**

Great news! It looks like Cybot has been using a hard drive to back up and store all his important files, including all the ones that we needed to solve the case! Now that we have this super-secret knowledge, Viro can't stop us from defeating them and we can save Cyber Agents headquarters from a malware attack.

Now that you're a cyber security expert, you can use your knowledge to protect your family from cyber criminals just like Viro.

Ask for a trusted adult's permission to visit GetCyberSafe.ca/Kids to see what else you can do to get cyber safe today!

Quiz Answers

Quiz 1: Passwords and passphrases

Question 1:

A Correct!

You should never share your passwords with anyone (unless it's your parent or guardian). You never know who might share them with someone else, so it's best to keep them top secret.

B Try again.

There are lots of secrets that you can share with your BFFs, but your passwords aren't one of them. Passwords help keep you safe online, so it's important to keep them to yourself.

C Try again.

A real bestie would never ask for your password because there aren't any good reasons they would need it. Your passwords help keep you safe online, so it's important to keep them to yourself.

Question 2:

A Try again.

Using the same password isn't a safe thing to do. If cyber criminals found out your password, they could hack all your accounts.

You can ask a parent or guardian to help you remember your passwords with a password manager.

B Correct!

You shouldn't use the same password more than once. If cyber criminals found out your password, they could hack all your accounts.

Question 3:

A Correct!

Passphrases are a type of password. They are long and secure while still being easier to remember than a bunch of random numbers and letters.

B Try again.

Short passwords may be easier to remember, but they won't do a great job at keeping you safe online. It's better to use a passphrase or a longer password instead!

C Try again.

Your pet's name may be easy for you to remember, but it is also easy for cyber criminals to guess. You should never use personal information, like your pet's name or your birthday, for your passwords.

Quiz 2: Tools

Question 1:

A Try again.

Saving a file twice on the same device won't protect it if your device gets lost, stolen or broken. You'll need to save it somewhere else that's just as secure.

B Correct!

The best way to back up a file is by saving it in another safe place, like a USB, a hard drive or in the cloud. That way, if something happens to your device, you'll have a backup of your file somewhere else!

C Try again.

Deleting important files will make you lose them! Try saving them somewhere else.

Question 2:

A Correct!

You can use multi-factor authentication (MFA) on your accounts and devices when you're trying to log in. It's an extra step you can take to prove your identity – like face ID or using a PIN on top of your passphrase!

B Try again.

Multi-factor authentication (MFA) IS a long word – but it's also much more than that! MFA is great for protecting you and your devices.

C Try again.

Believe it or not, multi-factor authentication (MFA) makes it much more difficult for cyber criminals to access your accounts compared to solving a riddle! MFA is a great way to protect you and your tools.

Question 3:

A Correct!

You should update your software as often as possible to make sure your devices are safe. Ask your parent or guardian to help you enable automatic updates, so your devices update by themselves!

B Try again.

If your phone or other devices are super slow, it might be a sign they need software updates. You should never wait until things slow down to update, though!

C Try again.

The easiest way to get rid of that pesky pop-up? Run the software update! The sooner you do it, the sooner the pop-up reminder will disappear.

Quiz 3: Wi-Fi/Networks

Question 1:

A Correct!

Software updates make your device more secure and when your device is more secure, so is everything it's connected to – including your Wi-Fi network!

B Try again.

Updating your devices is one of the easiest ways to stay cyber safe!

Question 2:

A Try again.

Leaving your router near the edge of your house could make it easier for strangers or cyber criminals to connect to it! Plus, the closer you are to your Wi-Fi signal, the stronger it is. Placing it closer to where you are is best.

B Correct!

Putting your router in the middle of your home can make it easier for you and your family to connect to it and more difficult for cyber criminals to access it!

C Try again.

Hiding stuff can be a good way to keep things safe, but not when it comes to your router. If your router is buried under your toys or hidden somewhere, it can be difficult for you and your family to connect to your Wi-Fi!

Question 3:

A Try again.

While this answer is true, it isn't the only reason. There's an even better answer.

B Try again.

While this answer is true, it isn't the only reason. There's an even better answer.

C Correct!

A lot of routers will have the same built-in password, and cyber criminals can easily crack them. Ask your parent or guardian if they've changed your Wi-Fi password.

Quiz 4: Phishing

Question 1:

A **Correct!**

You should never open messages from strangers online or click on any weird links or downloads from them. The best thing to do is not open the link, ask a trusted adult for help and delete the message.

B Try again.

Opening a message from someone you don't know could be dangerous. You could accidentally download a virus, or worse!

C Try again.

You should never forward a strange message to anyone else! Sending a bad message to a friend or family member could cause them to get a virus or lose their private information. The best thing to do is ask a trusted adult for help and delete the message.

Question 2:

A **Correct!**

Lots of people will hide their identity online and pretend to be someone they aren't. If you aren't sure whether someone is who they say they are, ask a trusted adult for help.

B Try again.

It can be hard to know whether someone is who they say they are when they're online because you can't see them in real life! Some people will pretend to be people you know. If you aren't sure, ask a trusted adult for help.

Question 3:

A Try again.

While spelling mistakes are one of the most common mistakes cyber criminals will make, it's not the only clue. There's a better answer.

B Try again.

Cyber criminals will often use email addresses that are random letters and numbers or even use their own personal email address to try and fool you, but it's not the only sign.

C Try again.

Cyber criminals want you to click on strange links or attachments to either get information from you or force you to download something bad, like a virus but it's not the only sign.

D **Correct!**

Spelling mistakes, a weird email address, and strange links and downloads are all signs of a phishing message. Be on the lookout when you get a message from someone you don't know.

Quiz 5: Malware

Question 1:

A Correct!

Backing up your data offline is a great way to save your most important files if they ever get lost or stolen.

B Try again.

Backing up your data offline can save your files, since all your important files are saved somewhere else, they won't be affected, and you can still restore them. That means you don't have to worry about losing them!

Question 2:

A Try again.

Malware can delete or steal your data. But data isn't the only thing malware can mess with.

B Try again.

Malware can do terrible things to your devices, like make them slower. But devices aren't the only thing malware can mess with.

C Try again.

Malware can do terrible things to your network, like steal your data and infect your devices. But networks aren't the only thing malware can mess with.

D Correct!

Malware is bad software that can harm all your data, devices, and networks.

Question 3:

A Try again.

You should never download something just because an email or text message asks you to, especially if it's from someone you don't know! Ask a trusted adult what to do and delete the message.

B Correct!

You should always ask a trusted adult before downloading anything online.

C Try again.

Even if something seems cool, that doesn't mean that it's cool to download. Ask a trusted adult before you download anything.

Glossary

Anti-virus software

A special type of software that defends against viruses. Anti-virus software uses a scanner to find programs that are or may be bad viruses on your computer or device.

Attachment

An attachment is a file that you upload. It can contain non-harmful files like pictures, videos, or documents, but it can also contain harmful files like malware and viruses.

Back up

A back up is when you make extra copies of data (like files, or software) in case the original is lost or damaged.

Cloud storage

Cloud storage is a way to save files, documents and photos to a server that isn't on or near your device. A cloud storage service may come with your computer or device.

Device

A device is an electronic tool like your phone, laptop, or tablet that you might use at home.

Download

A download is when you copy data from one device or system onto another device

Firewall

A security barrier that helps protect your devices from being accessed.

Hard drive (external)

An external hard drive is a device that you plug into your computer to help you store or backup data.

Malware

Malware stands for malicious software. It is made by cyber criminals to damage people's computers. Malware can do bad things to your devices like steal information, delete stuff from your devices, or pretend to be you.

Multi-factor authentication

Multi-factor authentication (MFA) adds an extra layer of security to your accounts and devices. MFA makes you add additional information to prove who you are – like a fingerprint, facial recognition, or a secret code like a PIN – to stop cyber criminals from getting into your accounts and devices.

Network

Several devices that are connected to one another, for example, a router, a phone, and a laptop.

Passphrases

A combination of random words you select to secure an account or device.

Passwords

A combination of letters and numbers you select to secure an account or device.

Password manager

A tool you can use to store all your passwords and passphrases, so you don't have to memorize them all yourself. It can help keep your passwords and passphrases safe, too.

PIN

A PIN is a Personal Identification Number. It is a passcode that only uses numbers and works like a password or a passphrase when you want to get access to an account or device.

Phishing

Phishing is an attempt by cyber criminal to steal information from an individual, group, or organization by pretending to be a specific, usually well-known brand. Phishing happens when cyber criminals want to steal information or money from you. They will pretend to be someone they aren't to trick you into giving them your information.

Router

A small device that connects our other devices, like tablets and phones, to the internet.

Software

A computer program that allows your device to work. Some common system softwares are ones that you're already familiar with, like Windows, Linux or Mac. Software can also be an application, like Microsoft Word or iMovie.

Update

Updates are done to software and devices to add new features and fix bugs or errors. They often contain new security features to protect against cyber attacks.

Wi-Fi

Wi-Fi allows your devices, like your laptop, tablet, and phone to connect to the internet. Using Wi-Fi at home is usually pretty safe since it's protected, but you should never connect to public Wi-Fi (like at the mall or a coffee shop) without a trusted adult's permission.
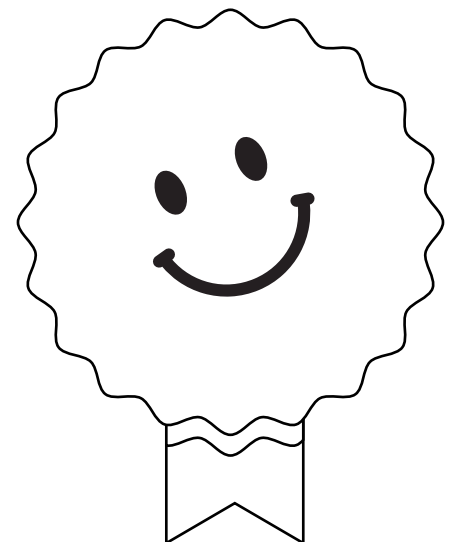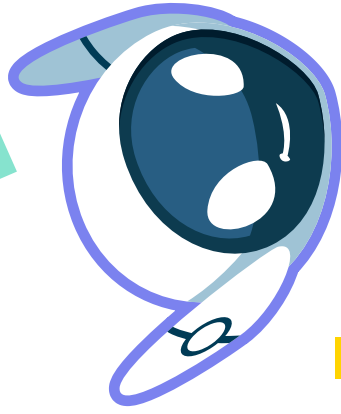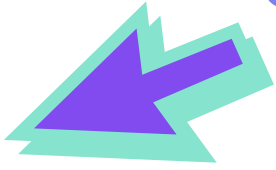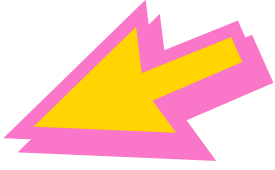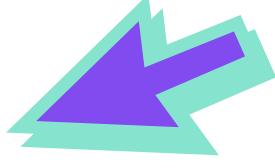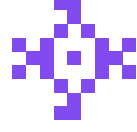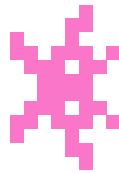
Certificate

of

Cyber Safety

This certificate is proudly presented to

for successfully completing cyber agent training.

Canada

GETCYBERSAFE.CA