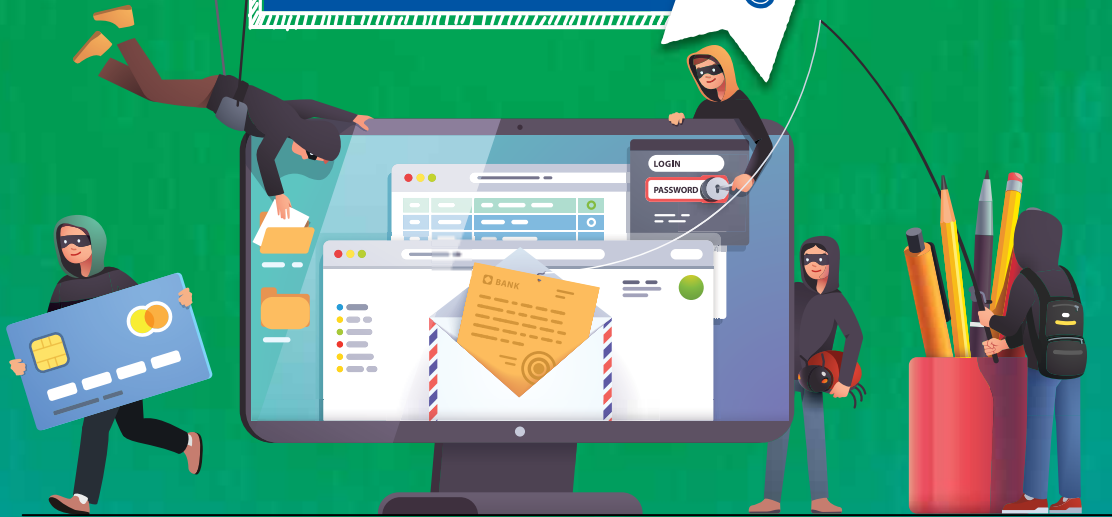


FINANCIAL and CYBER CRIME

AWARENESS

Family Activity Book 2.0



AFP

///JPC3

JOINT POLICING CYBERCRIME COORDINATION CENTRE



In the year 2000, less than 7% of the world were online and now over half the world's population (about 4 billion people) have access to the internet. The number of people using mobile phones has risen to the point where there are now more mobile phones in the world than people... Crazy but true.

The evolution of technology and the creation of the internet has provided us with unparalleled access to the world.

At the click of a button, we can access information, pay bills, buy goods, and share our stories with others and whilst this can make our lives easier, unfortunately it also creates opportunity for criminals.

With over 96% of Australians using the internet on a daily basis it provides the perfect environment for scammers to target us. Hands up everyone who has got an email or a text about an unexpected lottery win?

Technology has opened the world to us, but it has also opened us up to the world.

The police, government agencies, financial institutions, telecommunication companies and private industry are working together and have had some excellent results in identifying and stopping scammers, but the reality is that scammers will continue to change their tactics and will continue to take advantage of ever-evolving technology.

Their scams constantly change to match what is happening in our backyards.

So how do you protect yourself? Well, your best protection is education. Being aware of what is happening and applying some basic rules goes a long way to protecting yourself and your family from scams.

HERE ARE THE BASIC RULES:

STOP Don't give money or personal information to anyone if unsure

THINK Ask yourself could the message or call be fake?

PROTECT Contact your bank, report to ReportCyber and seek help from IDCARE.

- Never click on a link from an unknown email or text
- Never give out your personal information
- Never give out your banking details
- If you get an unsolicited call, just hang up
- If it's too good to be true, then it's probably a scam

Now of course we can't predict what our world will look like in another 10 years but with your help we can ensure that our future is one where we can access the world safely. This activity book is made for your family, and it's designed to be fun, but it is also our way of getting our message to the next generation. The sooner you can start the conversation with your children about internet safety the safer they will be.

THE JOINT POLICING CYBERCRIME COORDINATION CENTRE (JPC3)



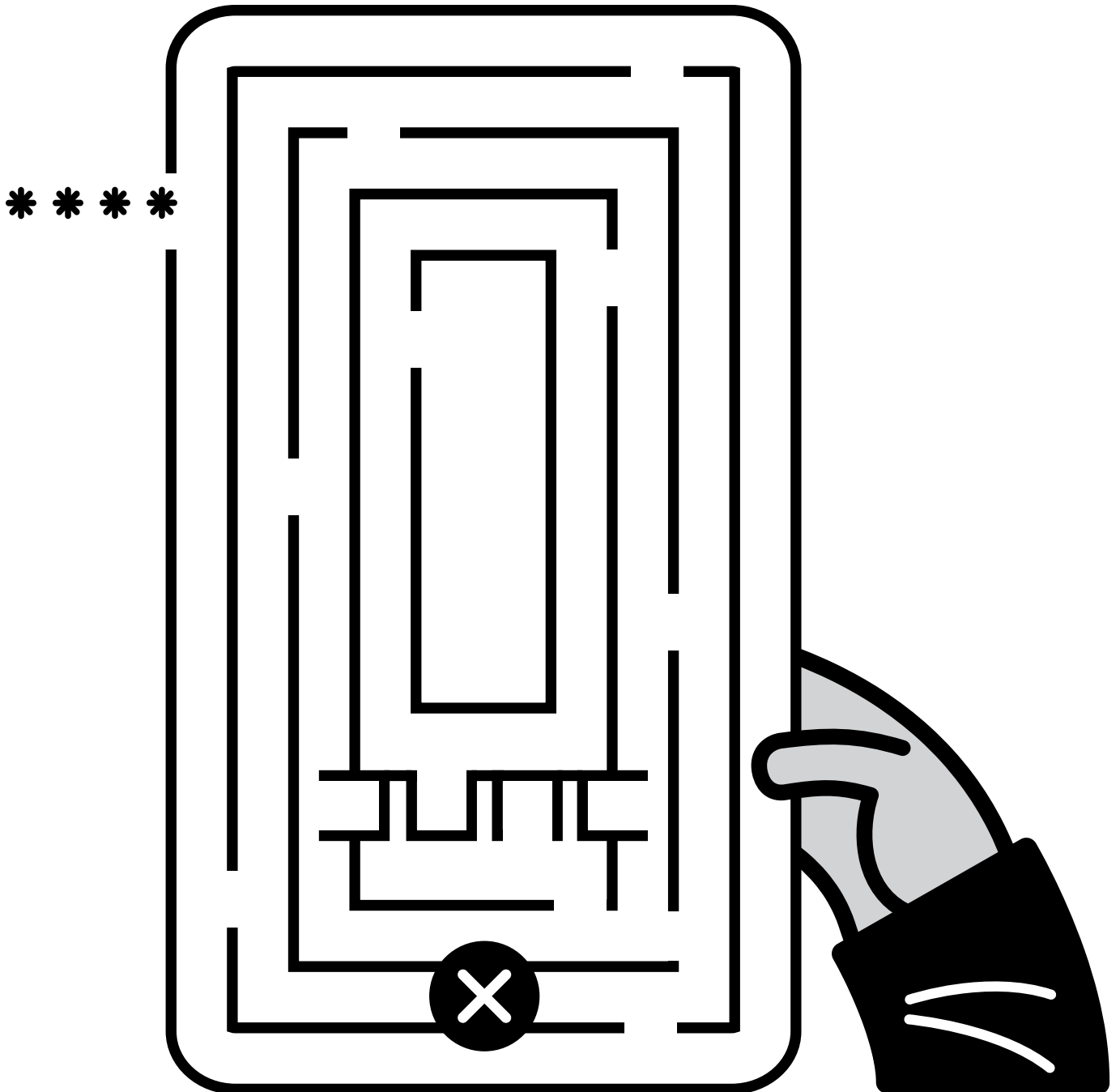
© Commonwealth of Australia 2024

With the exception of the Coat of Arms / logos of the AFP or any State or territory police force, and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution-NonCommercial 4.0 International licence (www.creativecommons.org/licenses). For the avoidance of doubt, this means this licence only applies to material in this publication. The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses). This publication also contains content prepared by the Queensland Police Service. Any attribution of this publication should be given to the Commonwealth of Australia and the Queensland Police Service.

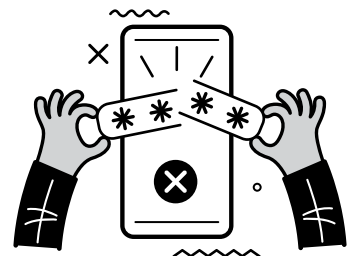
“Australian Law Enforcement respectfully acknowledge the Traditional Custodians of the lands, winds and water on which we so proudly serve our community. It is a privilege and honour to be on traditional country. We acknowledge Elders of the past, present and future, for they are the holders of culture, knowledge, wisdom and leadership that is passed from generation to generation. We acknowledge the significant contribution of Aboriginal People and Torres Strait Islander People toward the protection and safety of all people in this great country we live in and share”.

GET TO YOUR PHONE BEFORE THE HACKER...

Get each * to one of the four small boxes to complete the passcode.
Try not to use the same path.

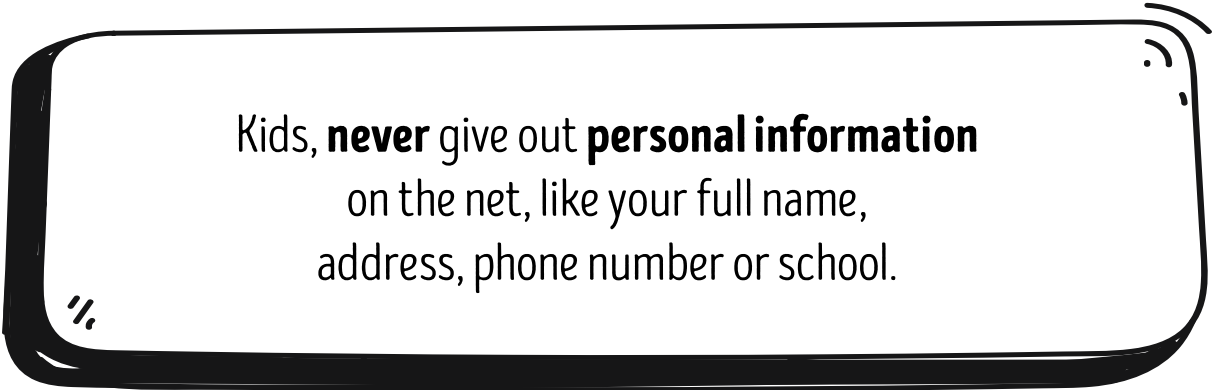


ARE YOU IN CONTROL...
...of your phone updates?

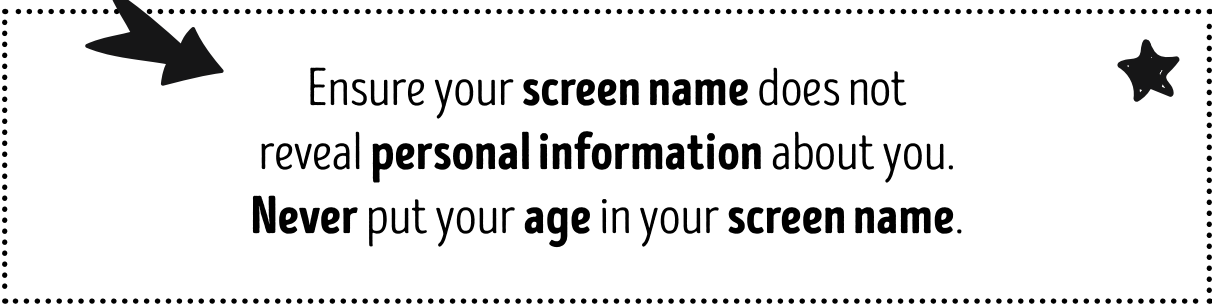


ONLINE SAFETY STAY AWARE

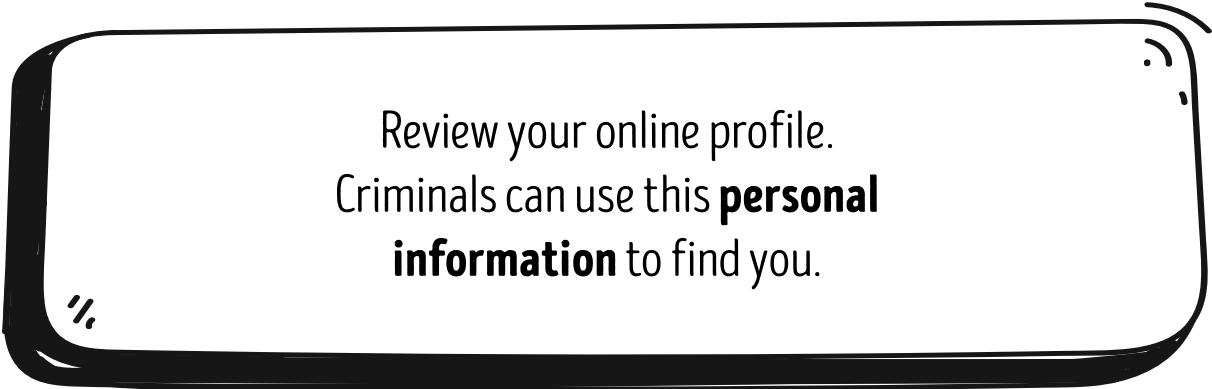
Anyone can fall victim to cybercrime.



Kids, **never** give out **personal information** on the net, like your full name, address, phone number or school.



Ensure your **screen name** does not reveal **personal information** about you.
Never put your **age** in your **screen name**.



Review your online profile.
Criminals can use this **personal information** to find you.

ARE YOU IN CONTROL...

...of the personal information you give out online?



**TIPS
#1**

CYBERCRIME WORD SEARCH

Never click on suspicious links.
You may be downloading malicious software.

WORDS TO FIND:

FIREWALL
CONTROL
PATCH
COOKIE

REPORTCYBER
ONLINE
HYPERLINK
RANSOMWARE

IOT
DEEPPFAKE
CYBERBULLYING
BOT

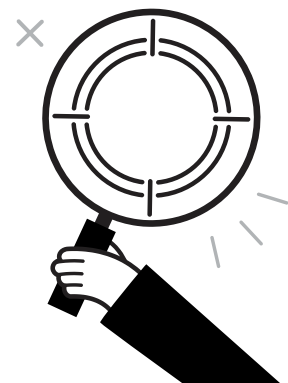
SCAREWARE
PASSPHRASE
HACKER
PRIVACY

PHISHING
SPYWARE
SCAMWATCH
MALWARE

HEYMUM
DATA
POLICE

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

ARE YOU IN CONTROL...
...of your online behaviour?



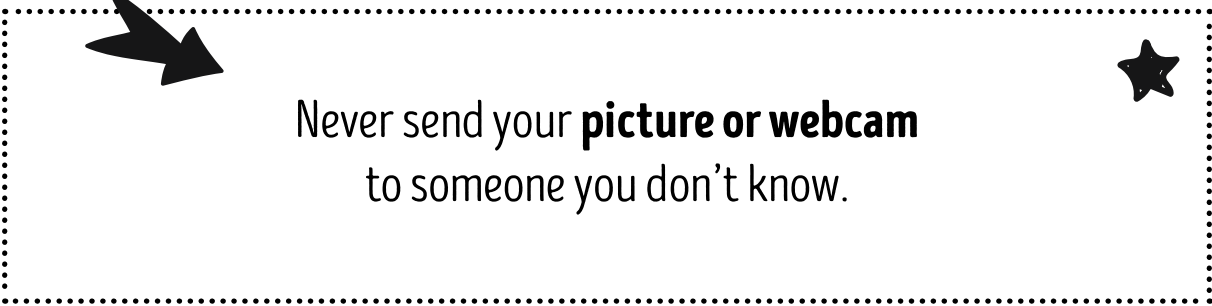
ONLINE SAFETY

DON'T CHAT TO STRANGERS

Be aware that there are dangerous people that try to be your friend on the internet.



Secure your online profiles to only allow **trusted friends** to view your content.



Never send your **picture or webcam** to someone you don't know.



Don't accept invitations from **randoms**.

ARE YOU IN CONTROL...
...of who you chat to online?



TIPS
#2

IS YOUR PASSPHRASE STRONG ENOUGH?

A strong passphrase should include four random words. Some online accounts require complex passphrases that include uppercase, numbers and symbols.

- **Uppercase:** ABCDEFGHIJKLMNOPQRSTUVWXYZ
- **Lowercase:** abcdefghijklmnopqrstuvwxyz
- **Numbers:** 1234567890
- **Symbols:** !@#\$%^&*()_+={}[?/.,
- **Strong passphrases look like this:** sky pink cake smelly
- **Complex passphrases might look like this:** Skyp1nk-Cakesmelly
- **Poor passphrases look like this:** mynameisclaire

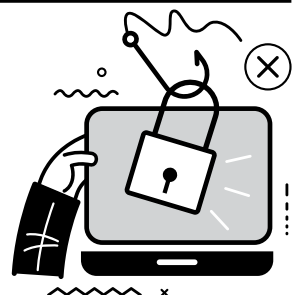


KEEP IT
SAFE



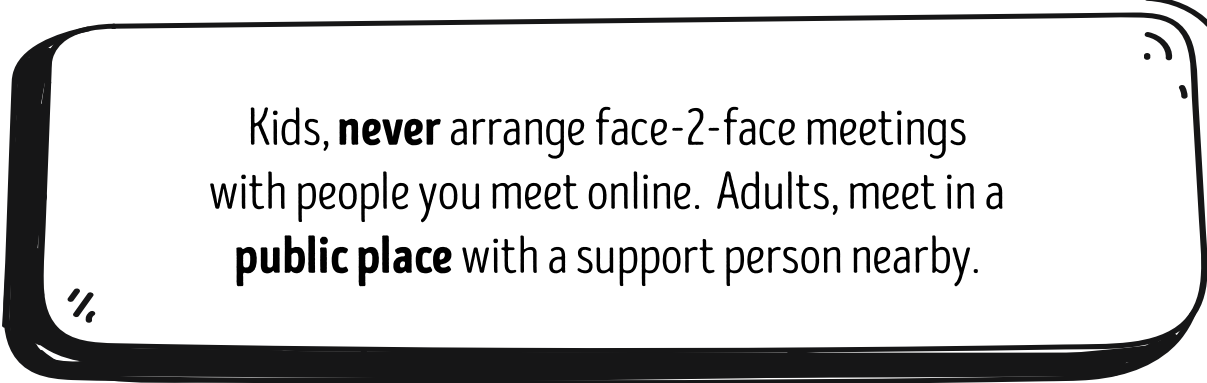
ARE YOU IN CONTROL...

...of your passphrase strength?

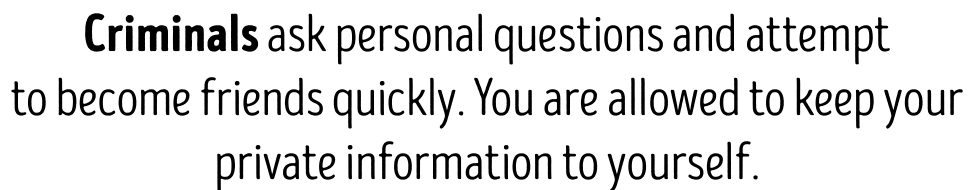


ONLINE SAFETY STAY AWARE

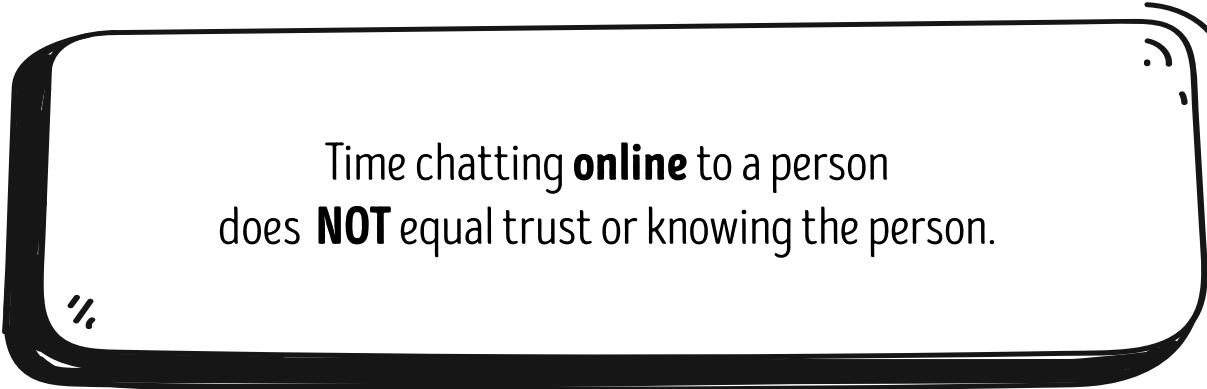
You are allowed to end a conversation if you feel uncomfortable or you are pressured to do something. It is okay to hang up and stop any communication.



Kids, **never** arrange face-2-face meetings with people you meet online. Adults, meet in a **public place** with a support person nearby.



Criminals ask personal questions and attempt to become friends quickly. You are allowed to keep your private information to yourself.



Time chatting **online** to a person does **NOT** equal trust or knowing the person.

ARE YOU IN CONTROL...
...of who you trust online?



**TIPS
#3**

CODE CRACKER

Malware is a term for any malicious software that can be installed on your computer or other devices.

Do not open attachments or click on links in emails or social media messages you've received from strangers - just press delete.

Decode the secret message.

The secret message is written in symbols. In the code key at the bottom of the page you can find what each symbol means. Write the letter above the symbol and you can read the secret message.

Good luck!

CODE KEY:

a	b	c	d	e	f	g	h	i	j	k	l	m
□	◆	△	◐	♣	➤	▼	♥	✕	◀	+	●	★
n	o	p	q	r	s	t	u	v	w	x	y	z
☆	*	◆	♠	♣	○	▲	■	◇	✱	◐	❖	⊕

 ■ ○ ♣ □ ◐ ✕ ➤ ➤ ♣ ♣ ♣ ☆ ▲

 ◆ □ ○ ○ ◆ ♥ ♣ □ ○ ♣ ➤ * ♣ ♣ ◇ ♣ ♣ ❖

 □ ◆ ◆ □ ☆ ◐ ▼ □ ★ ♣ ❖ * ■ ♥ □ ◇ ♣

 * ☆ ❖ * ■ ♣ △ * ★ ◆ ■ ▲ ♣ ♣

 □ ☆ ◐ ◆ ♥ * ☆ ♣

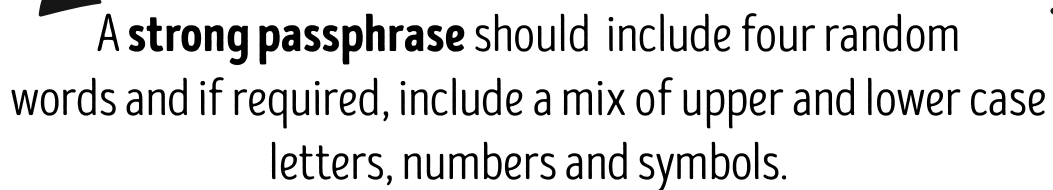
ARE YOU IN CONTROL...
...of your privacy settings?



ONLINE SAFETY PASSPHRASES

Do not allow remote access to your computer from people you meet online and remember, even 'friends' can be dangerous.

Keep your personal details **secure**.
Use a **Password Manager**.



A **strong passphrase** should include four random words and if required, include a mix of upper and lower case letters, numbers and symbols.

Kids, **don't** use the same passphrase for every account/profile. **Don't** share your passphrases with anyone except your parent or caregiver.

ARE YOU IN CONTROL...

...of what you think is a strong passphrase?



**TIPS
#4**

ONLINE SAFETY PASSPHRASE CHALLENGE

Circle the seven strong or complex passphrases below!

kYb}ih1HH^n_Uu-*4	QWERTY	pen letter bag lolly
fighter positive ranch colonel	q2edvMCWAX8whUDfDFdA	Em3ik#H8w}mi+7!e%
kevin	head salt tea laptop	BUNrQ7Ze:f?z-0r>g
CPS>:Q#^01:hh	cricket	:3ArNXRule?r
Password	Starwars	wastrel martyr vertex chateaux
sky-blue-sing-bell	play-TV-bottle-apple	Apple
	Password11	River m0use fork b!n

5 WAYS TO KEEP GAMING FUN:



1. Block, report and mute people who troll or bully you in games.
2. Take short breaks if you're gaming for a long time.
3. Don't share personal information with people in games.
4. Avoid in-game purchases like loot boxes.
5. Check the age rating of any games you play.



ARE YOU IN CONTROL...

...of who can see you when you are online?



CYBERCRIME WORD SCRAMBLE

Unscramble the letters to make the correct words below.
Draw a line to the unscrambled word.

MYEMHU

TEPNYMA

OURDEVE

DFAUR PEMTDERATN

YRRPTUOERNCCYC

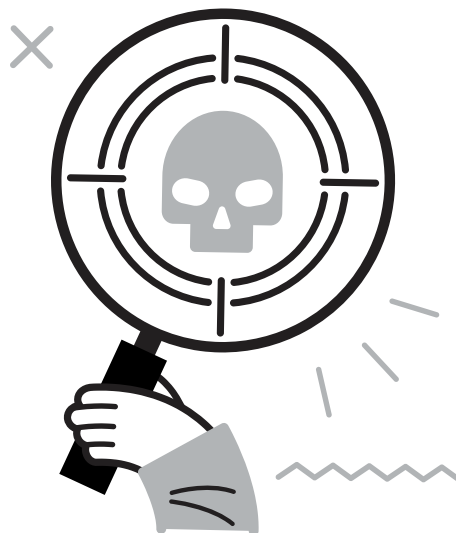
FKAE HYTRAIC

UTLBOF

ACREOMN

HIRIAENCENT

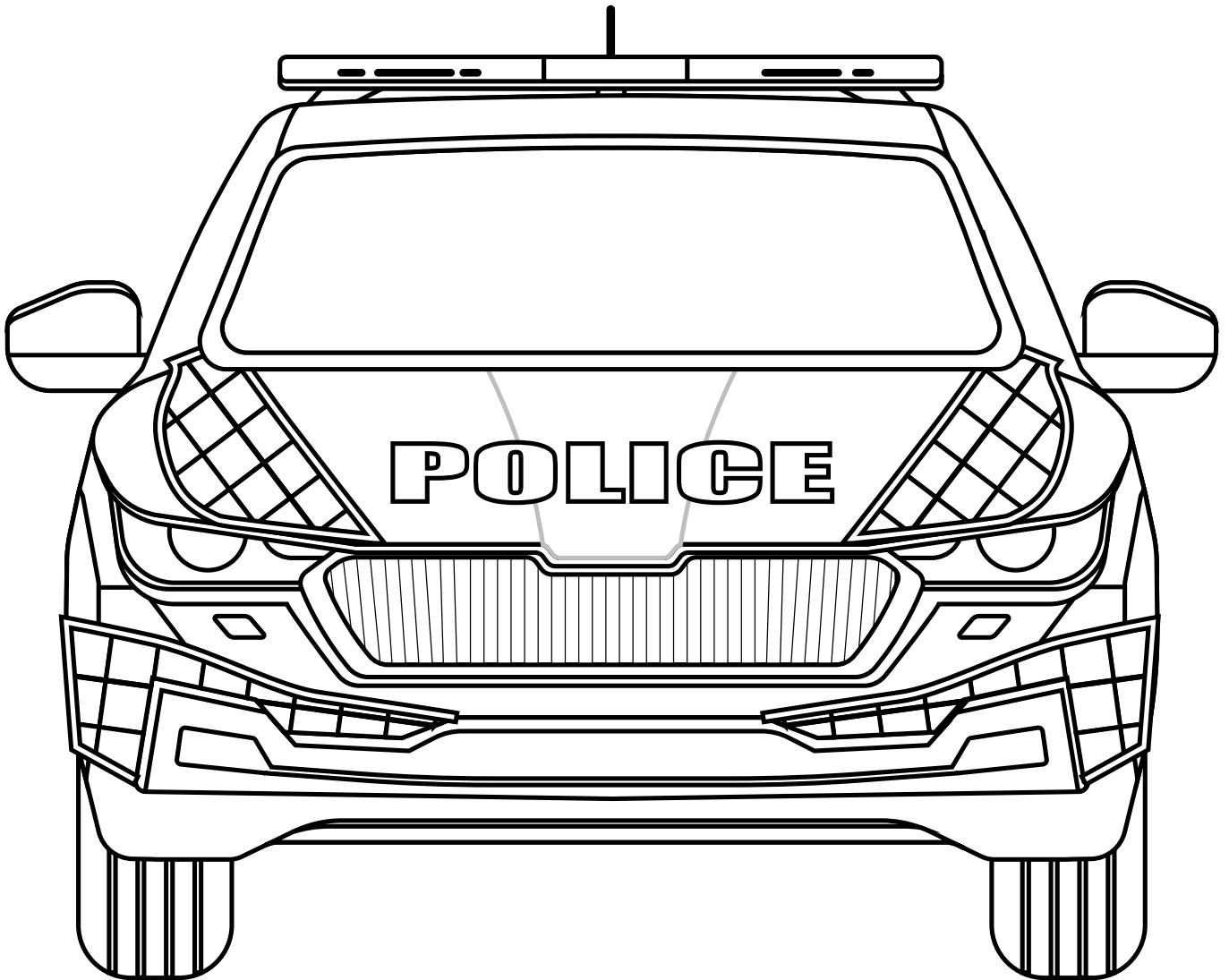
TOLTO



ARE YOU IN CONTROL...

Consider disabling location services on your apps and devices.

POLICE PATROL CAR COLOURING IN



ARE YOU IN CONTROL...
Keep selfies to yourself.



ONLINE SAFETY STAY AWARE

Cyber criminals can contact you by message, like text/SMS, social media platforms, and messaging apps.

Do not open **suspicious messages**, pop-up windows or emails. **Delete them.**

Can you find the suspicious text/SMS in this book?



Cyber criminals will **pretend** to be something and someone they are **NOT**.

Remember: Keep your personal details to yourself and keep them secure.

ARE YOU IN CONTROL...
...of what links you click on?



**TIPS
#5**

HOW MUCH DO YOU KNOW?

Use the words supplied below to fill in the best answer for each question.

1. Restrict the personal that you put online.
2. Use different for each of your social media sites.
3. Kids should never give out any information online
4. If you receive a phone call from an unknown person saying your is broken do not give them to it.
5. Do not open or click on in emails or social media messages you've received from strangers - just press
6. Stop and think before filling in online or entering online
7. love to create a sense of urgency - Don't feel pressured to act.



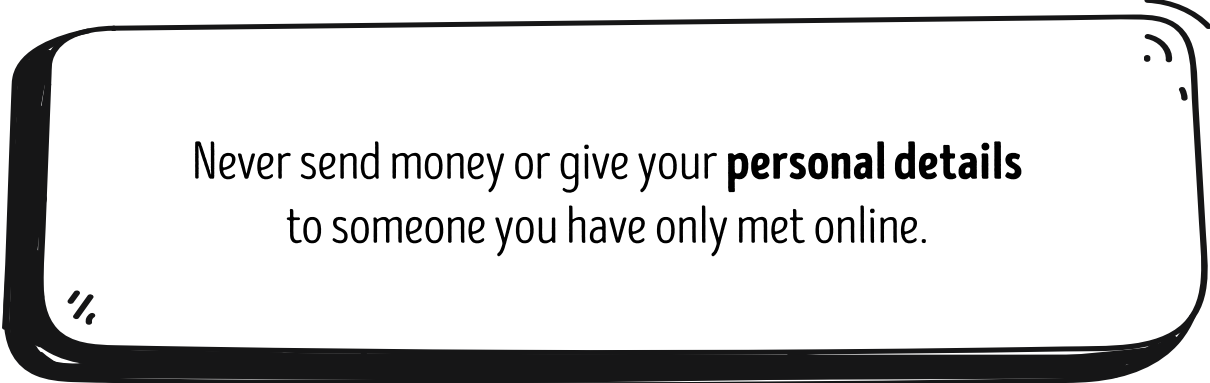
ARE YOU IN CONTROL...

...of what to do if you receive an 'URGENT' text from an unknown person?



ONLINE SAFETY PROTECT YOUR MONEY

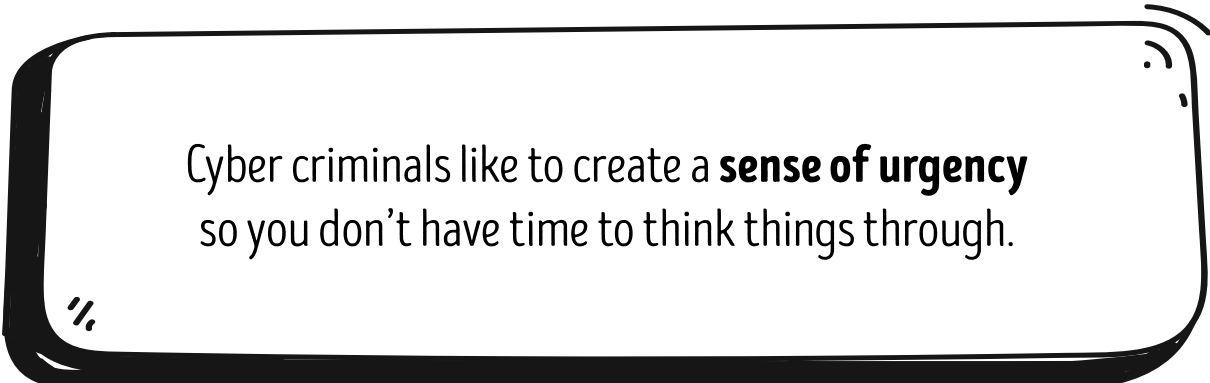
Never give out any personal information



Never send money or give your **personal details** to someone you have only met online.



Don't feel or be pressured into paying money.



Cyber criminals like to create a **sense of urgency** so you don't have time to think things through.

ARE YOU IN CONTROL...

Never send money to someone you just met online.



TIPS
#6

ONLINE SAFETY WORD SEARCH

Never provide your banking, financial and account details to someone that contacts you unexpectedly and that you don't know and trust.

WORDS TO FIND:

PARENTS
PASSWORD
COPYRIGHT

PERSONAL
HISTORY
REPORT

EMAIL
PERMISSION
SPAM

SECURE
CYBERCRIME
PREDATORS

INFORMATION
DOMAIN
FIREWALL

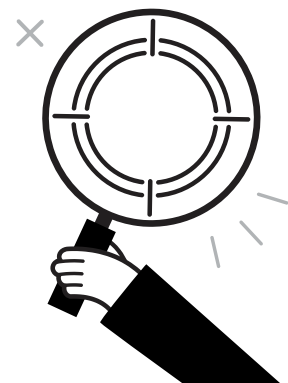
ADDRESS
DOWNLOAD
DIGITAL

BULLY
PRIVACY

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

ARE YOU IN CONTROL...

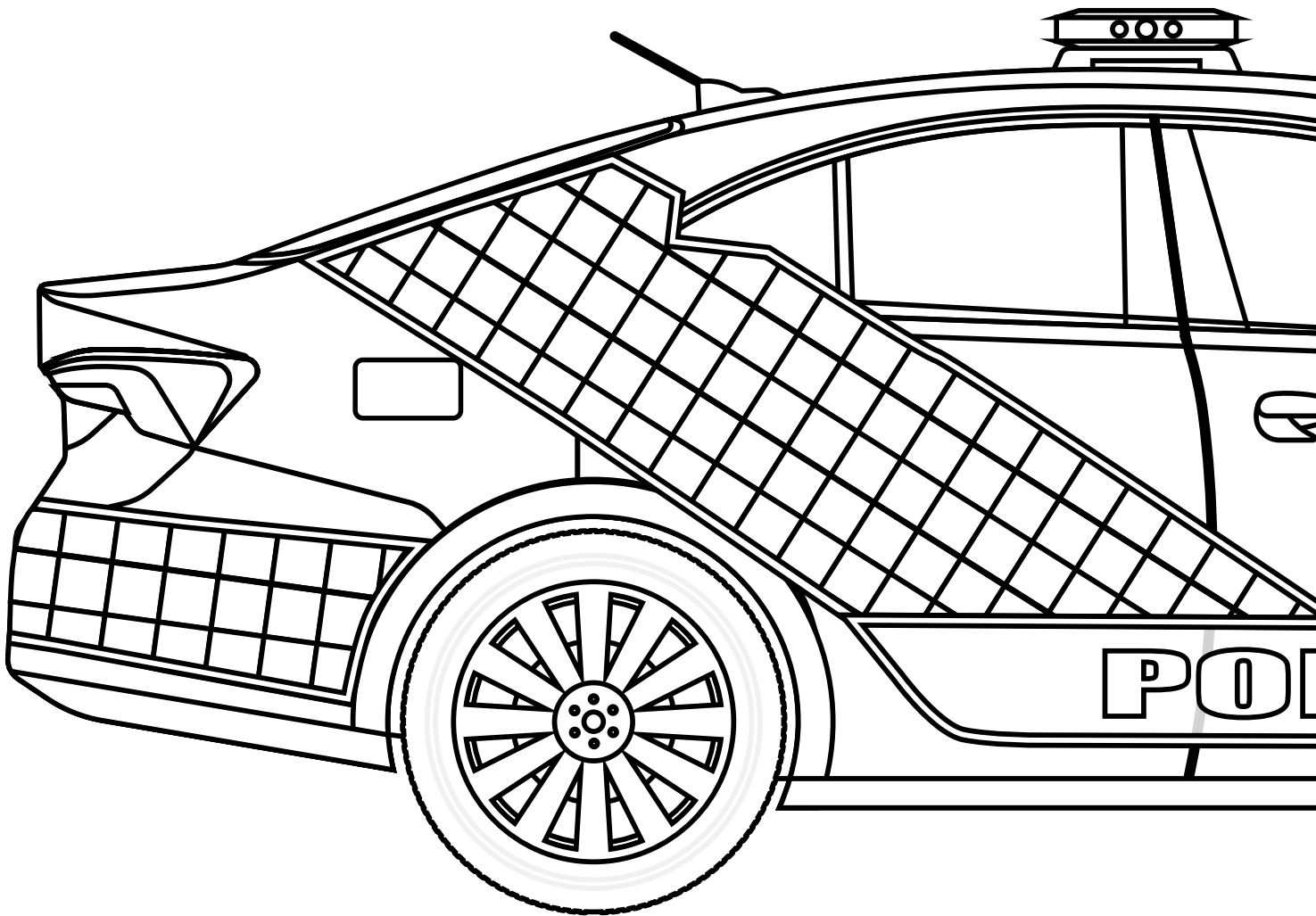
Be aware what kind of scams are out there.



FAMILY CODE WORD

Does your family have a code word that only you and your family know?

Cyber criminals may pretend to be a family member, the codeword can be used to verify identities.
This word needs to be easy to remember, say and type.

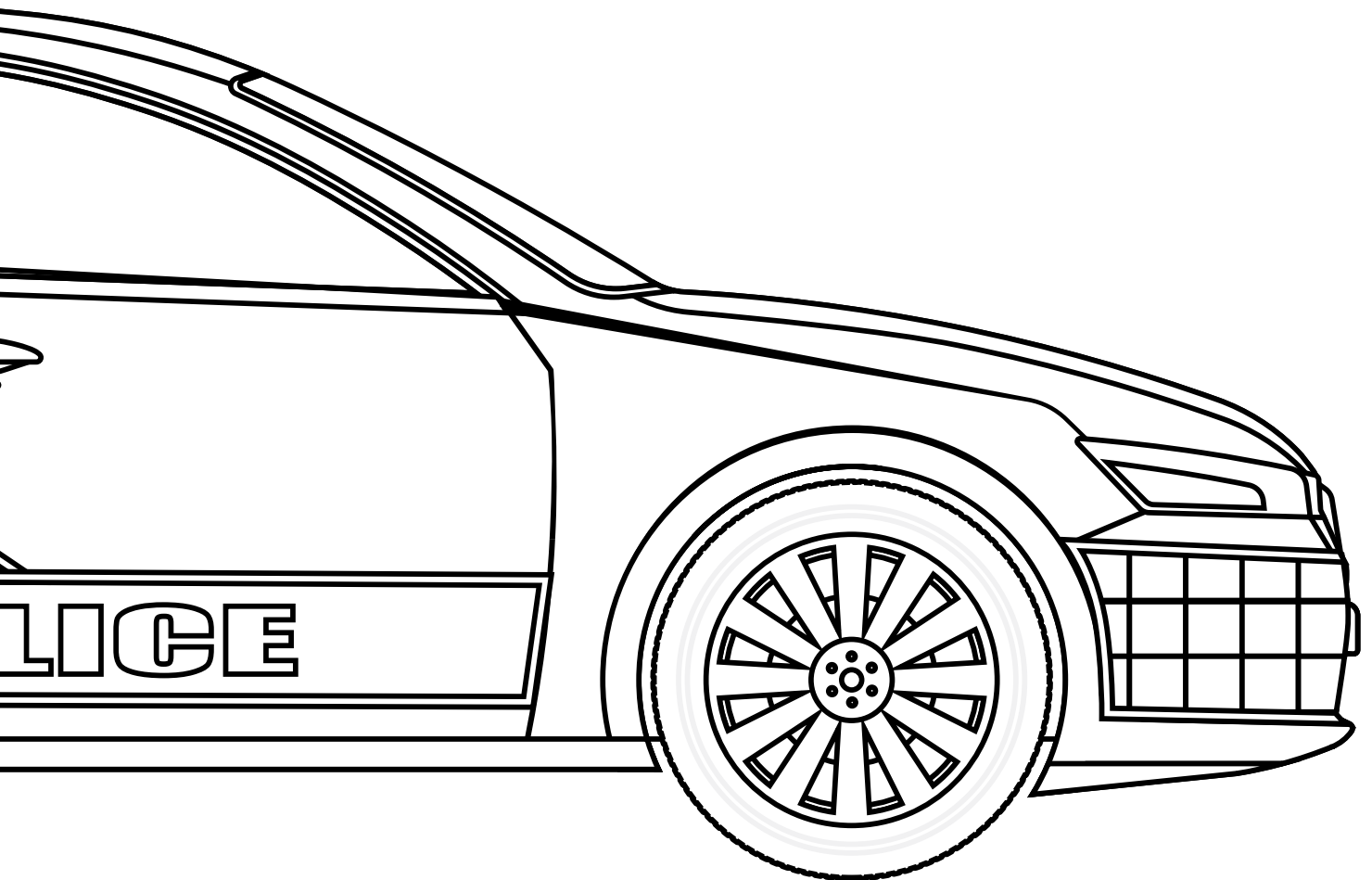


ARE YOU IN CONTROL...

If you need to contact the police in an emergency dial 000 and ask for the police.

HOW CAN YOU IDENTIFY PEOPLE YOU CAN TRUST?

Do you know the colours on our patrol cars?



ARE YOU IN CONTROL...

If you need to call the police but it's not an emergency call 131 444.

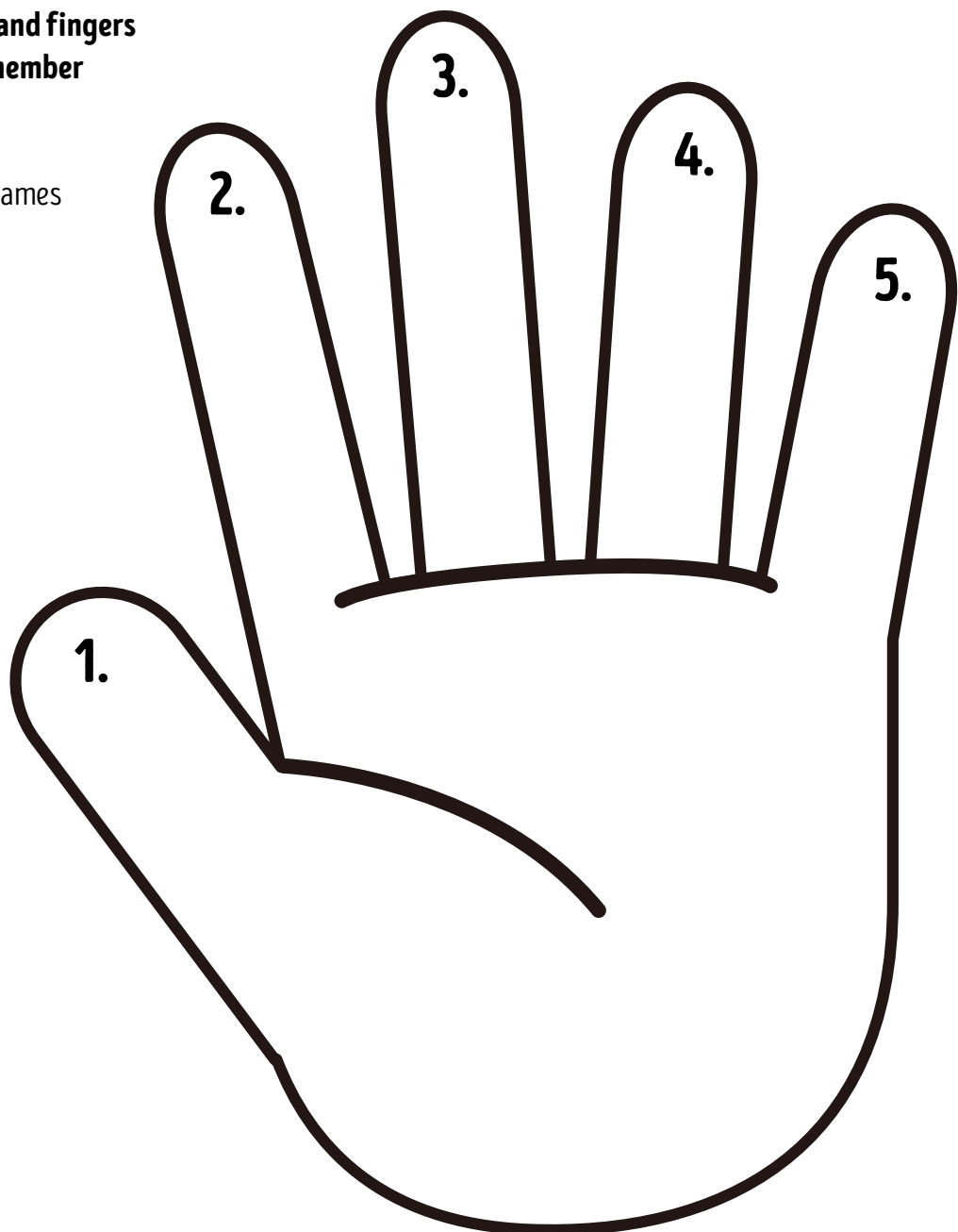


List 5 people you can trust and speak to if you are worried or in trouble.

1. _____
2. _____
3. _____
4. _____
5. _____

**Use your hand and fingers
to help you remember
who they are.**

Now write the names
on the fingers:



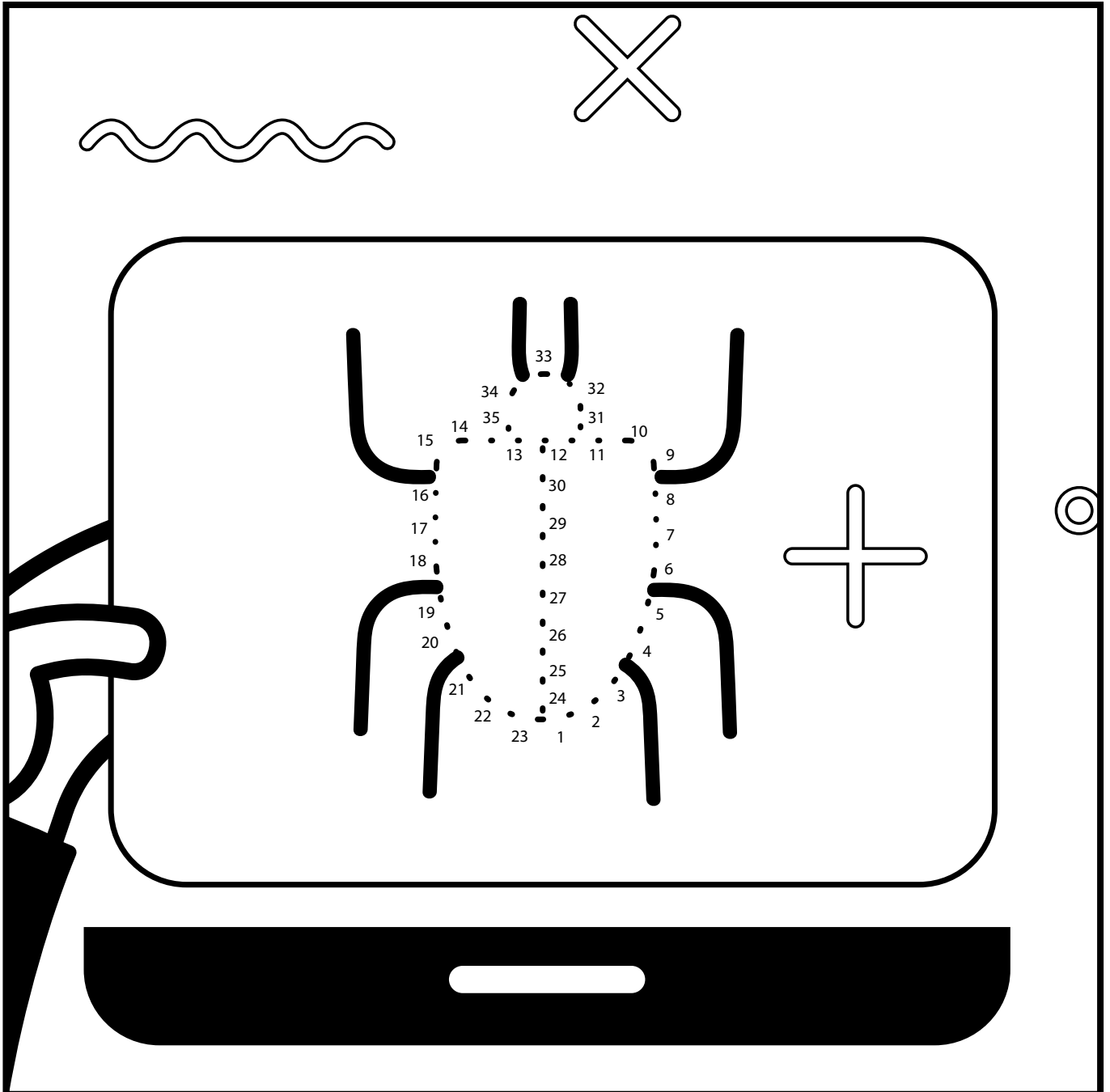
ARE YOU IN CONTROL...

Know who to call if you're in trouble.

CYBERCRIME DOT-TO-DOT

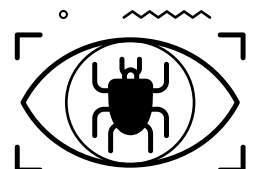
What could this possibly be?

Don't forget to turn on automatic updates and keep your anti-virus software up-to-date!

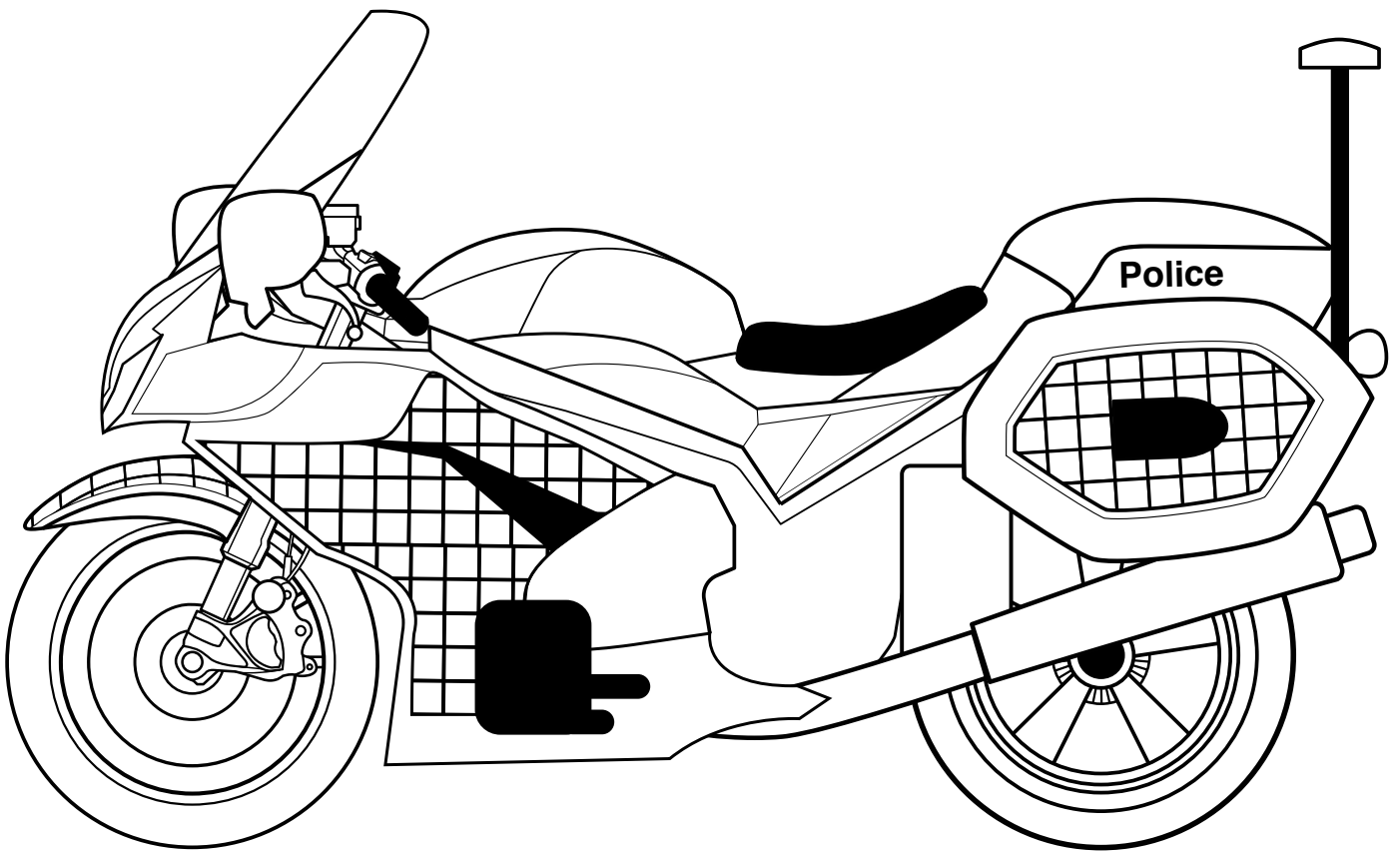


ARE YOU IN CONTROL...

Set up automatic updates on your devices.



POLICE MOTORBIKE COLOURING IN



ARE YOU IN CONTROL...

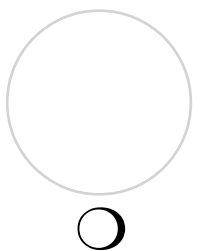
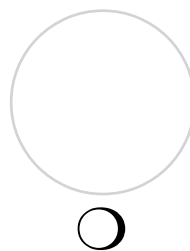
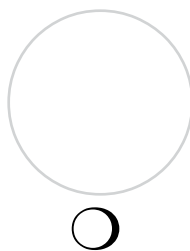
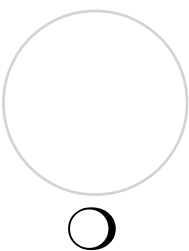
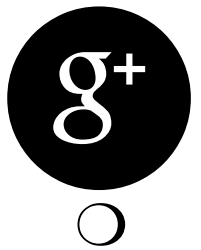
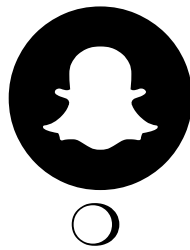
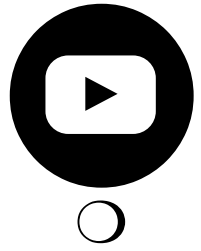
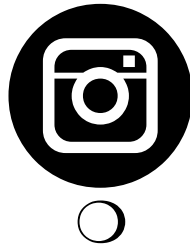
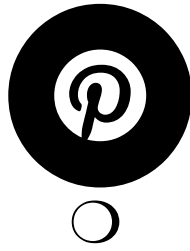
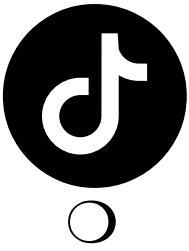
Be aware that scammers like gift cards as payment.

CHECK YOUR APPS WHICH ONES DO YOU HAVE?

Check your App permissions, don't share your location with randoms.

Can you name these Apps?

Tick the circle if you have checked your privacy settings.



Draw other Apps you use in the spaces above.

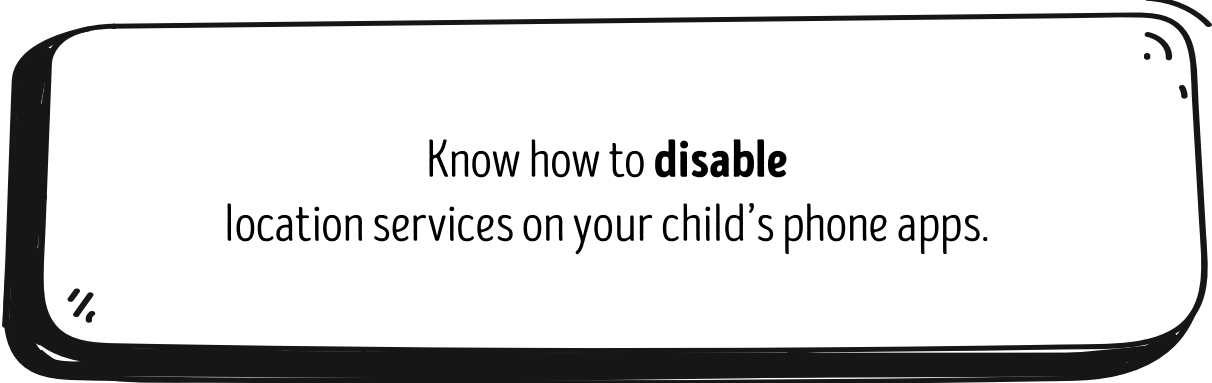
ARE YOU IN CONTROL...
...of your privacy settings?



ONLINE SAFETY PROTECT YOUR MONEY

Cyber criminals are willing to accept money by any means...

... this can include gift cards, Google Play, Steam, or iTunes cards.



Know how to **disable**
location services on your child's phone apps.



Change your **passphrases** frequently.



Don't send money to someone
you have only met **online** or over the **phone**.

ARE YOU IN CONTROL...

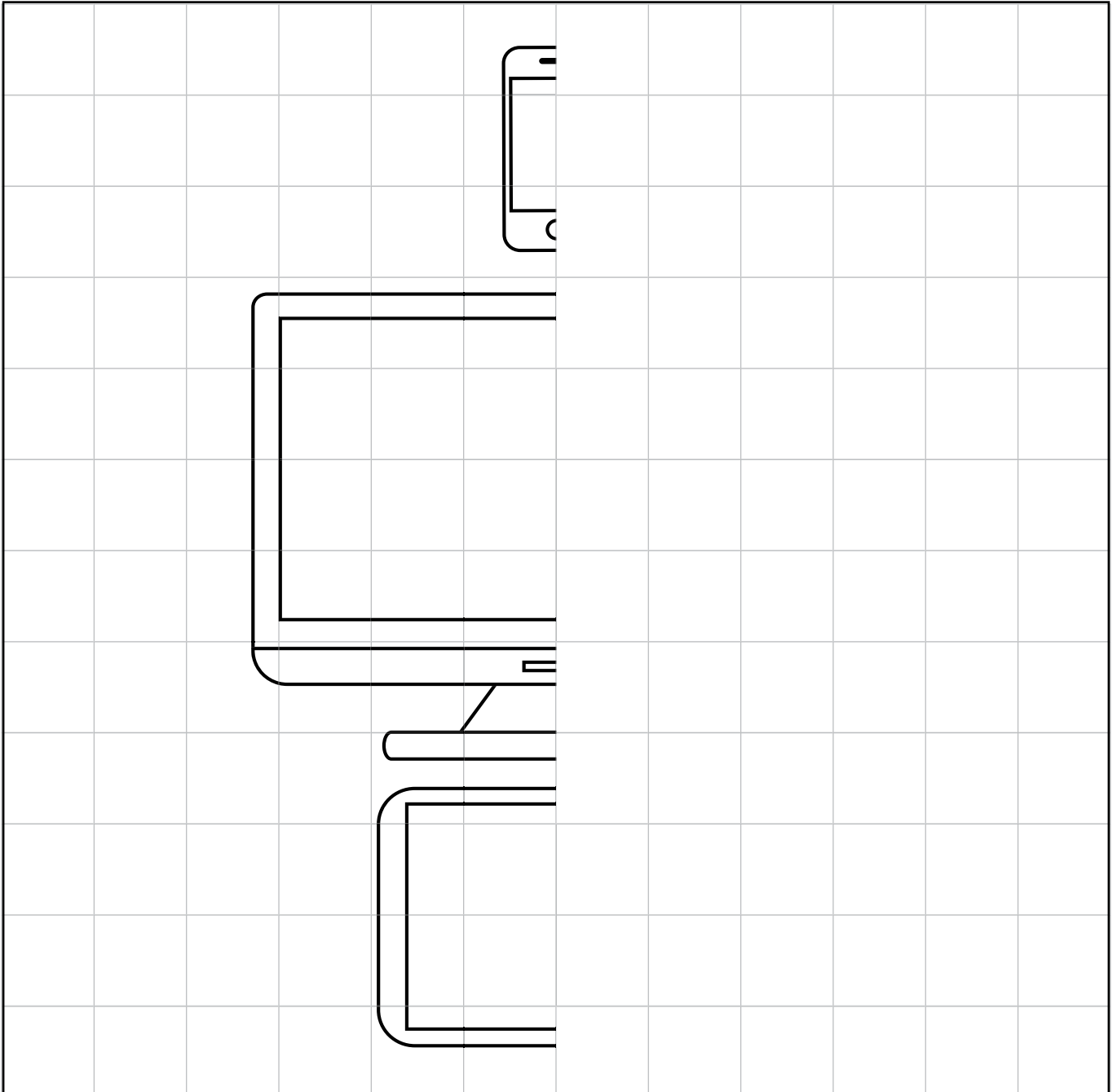
Monitor your child's phone for unusual activity.



TIPS
#7

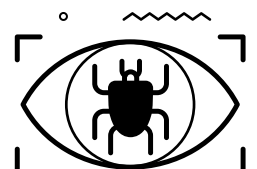
COMPLETE AND COLOUR CHECK ALL YOUR DEVICES!

Turn on multi-factor authentication (MFA) on all your devices and accounts to add an extra layer of security. Examples include Face ID or a code sent to you via SMS or email.



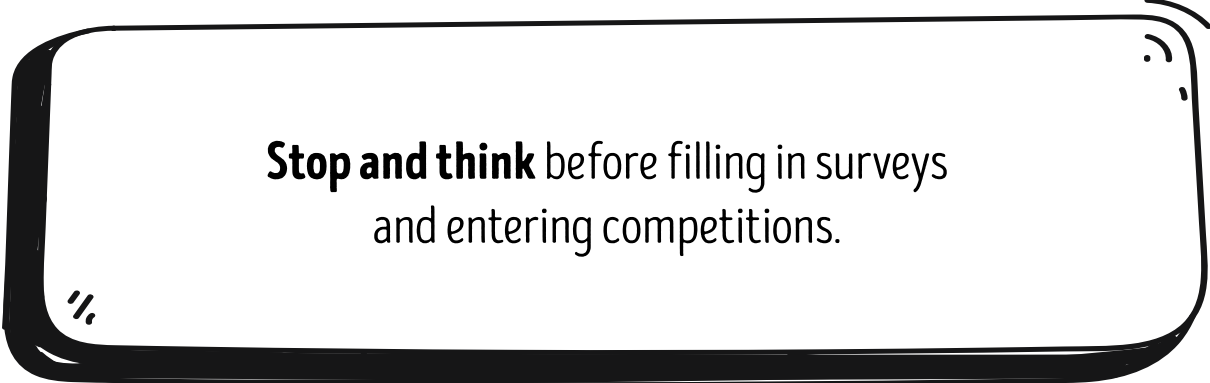
ARE YOU IN CONTROL...

Only accept friend requests from people you know and trust.




ONLINE SAFETY STOP AND THINK

Cyber criminals like to create a sense of urgency.
Think before you click.



Stop and think before filling in surveys
and entering competitions.



Stop and think before clicking on links
or attachments. Is the message real?



Stop and think before
'befriending', 'liking' or 'sharing' something online.

ARE YOU IN CONTROL...

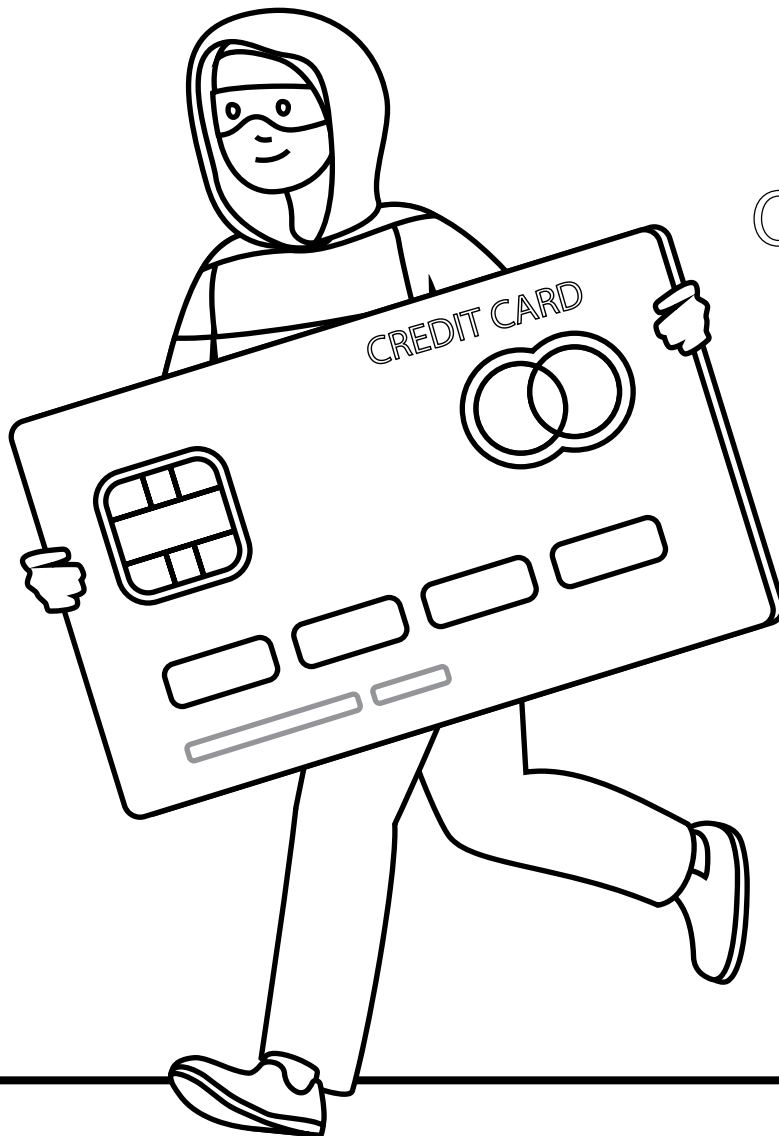
Use different passphrases for all online accounts.



TIPS
#8

CYBER SAFETY COLOURING IN

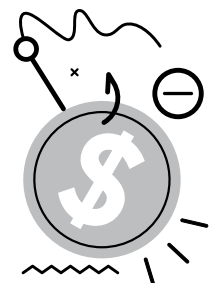
KEEP IT
SAFE
ONLINE



USE MULTI-FACTOR AUTHENTICATION

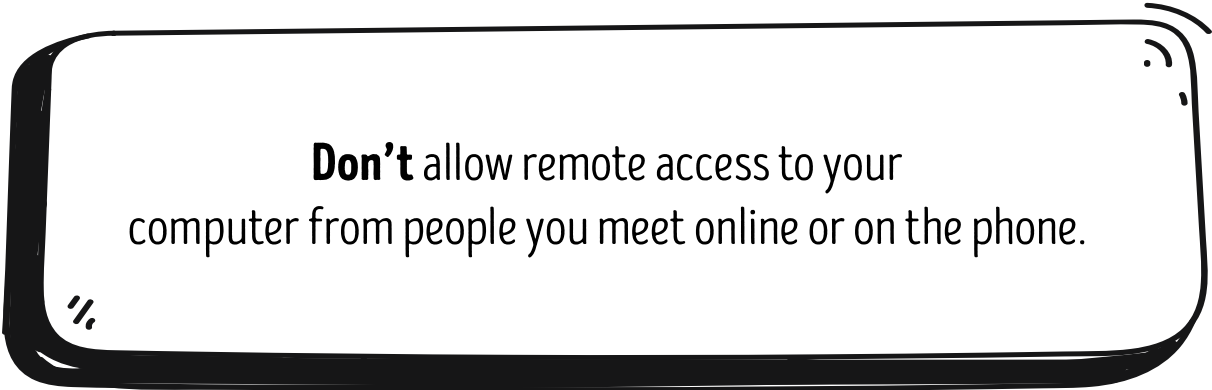
ARE YOU IN CONTROL...

Use multi-factor authentication.



ONLINE SAFETY STOP AND THINK

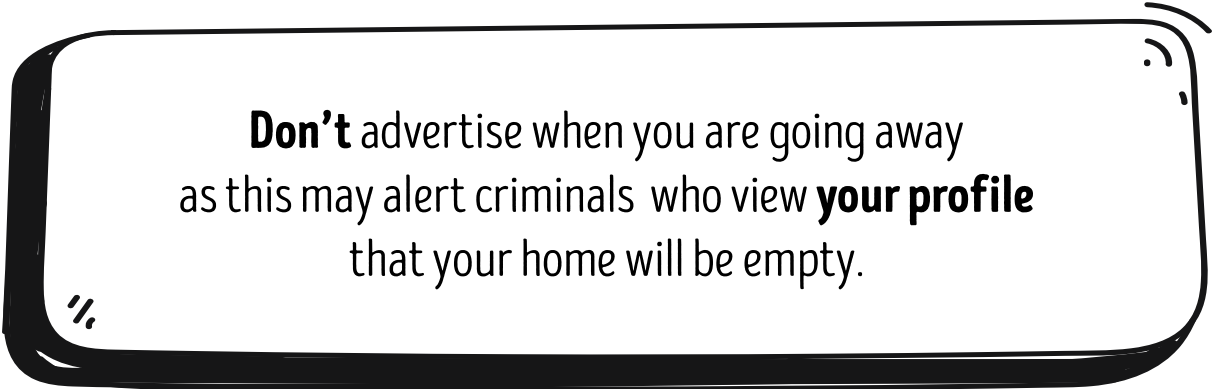
Remember, friending a stranger online is the same as giving an unknown person in the street details about your life.



Don't allow remote access to your computer from people you meet online or on the phone.



Restrict the personal information you put online.



Don't advertise when you are going away as this may alert criminals who view **your profile** that your home will be empty.

ARE YOU IN CONTROL...

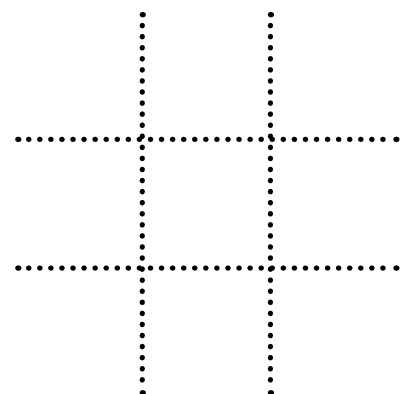
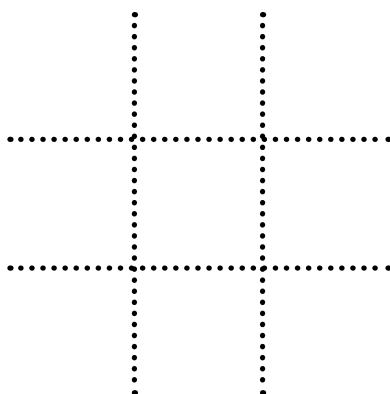
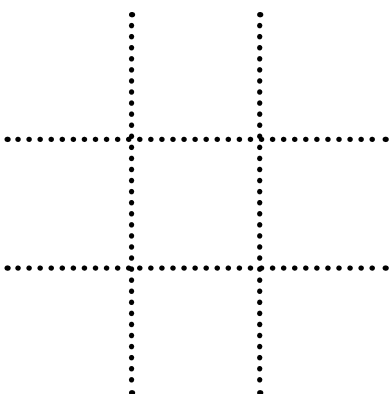
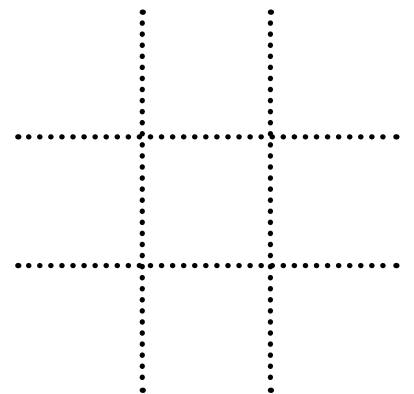
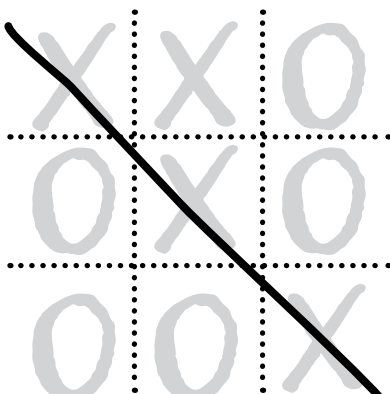
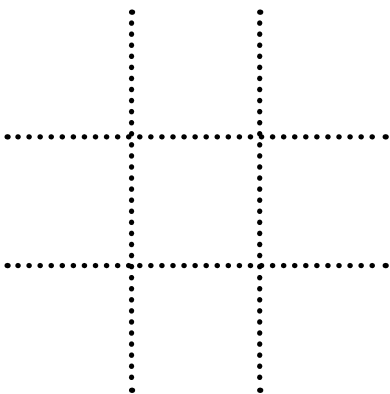
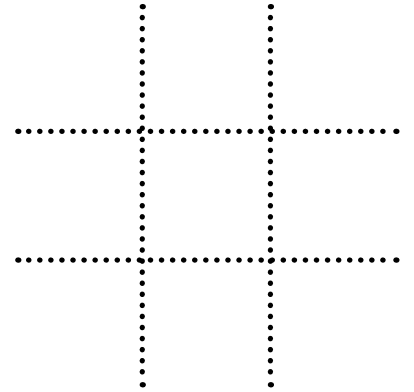
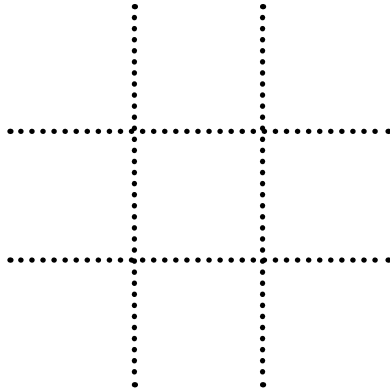
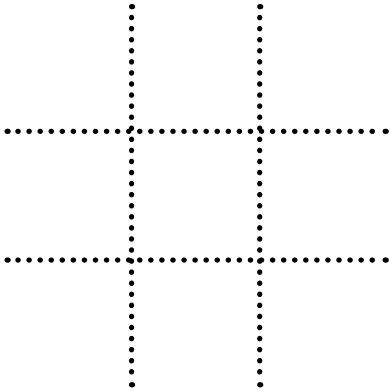
Microsoft will never ring you to say your computer has a virus or any other problem.



TIPS
#9

GAME OF NOUGHTS & CROSSES

Two players. One player is nought (O), the other a cross (X).
Take turns. The first to get a line of three noughts or crosses wins.



ARE YOU IN CONTROL...

Never tell anyone your passphrase or login codes.

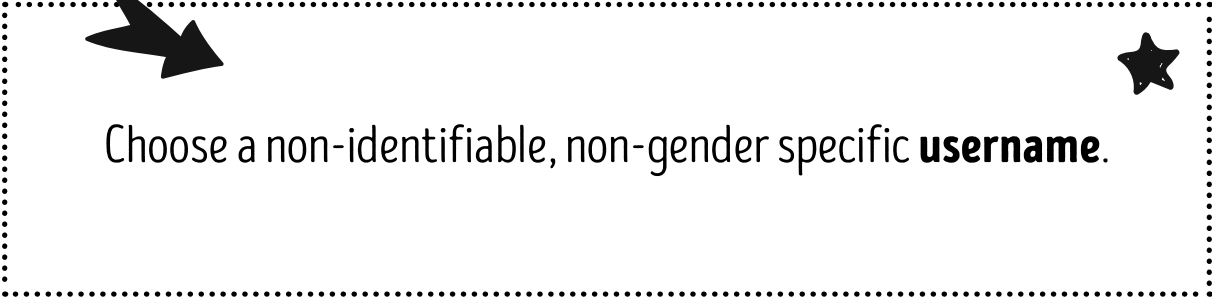


ONLINE SAFETY STAY AWARE

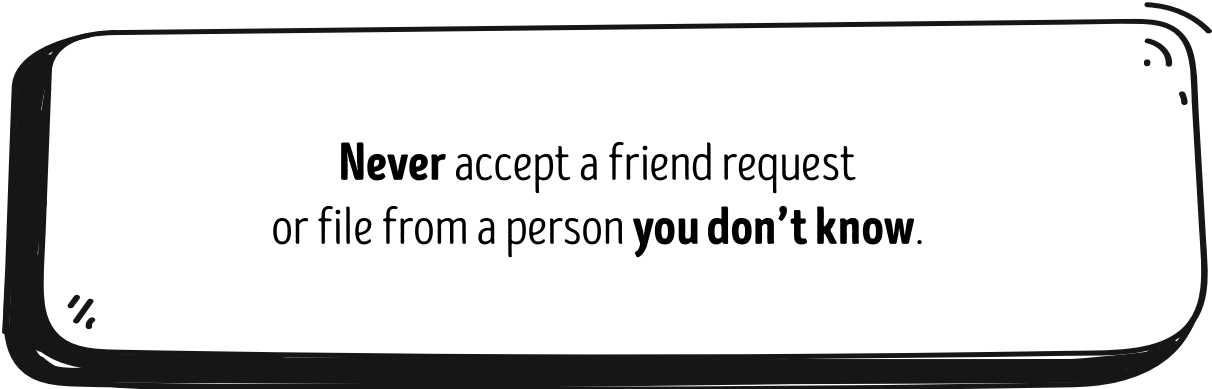
DO NOT share passphrases.



Use **different passphrases**
for each of your social media accounts.



Choose a non-identifiable, non-gender specific **username**.



Never accept a friend request
or file from a person **you don't know**.

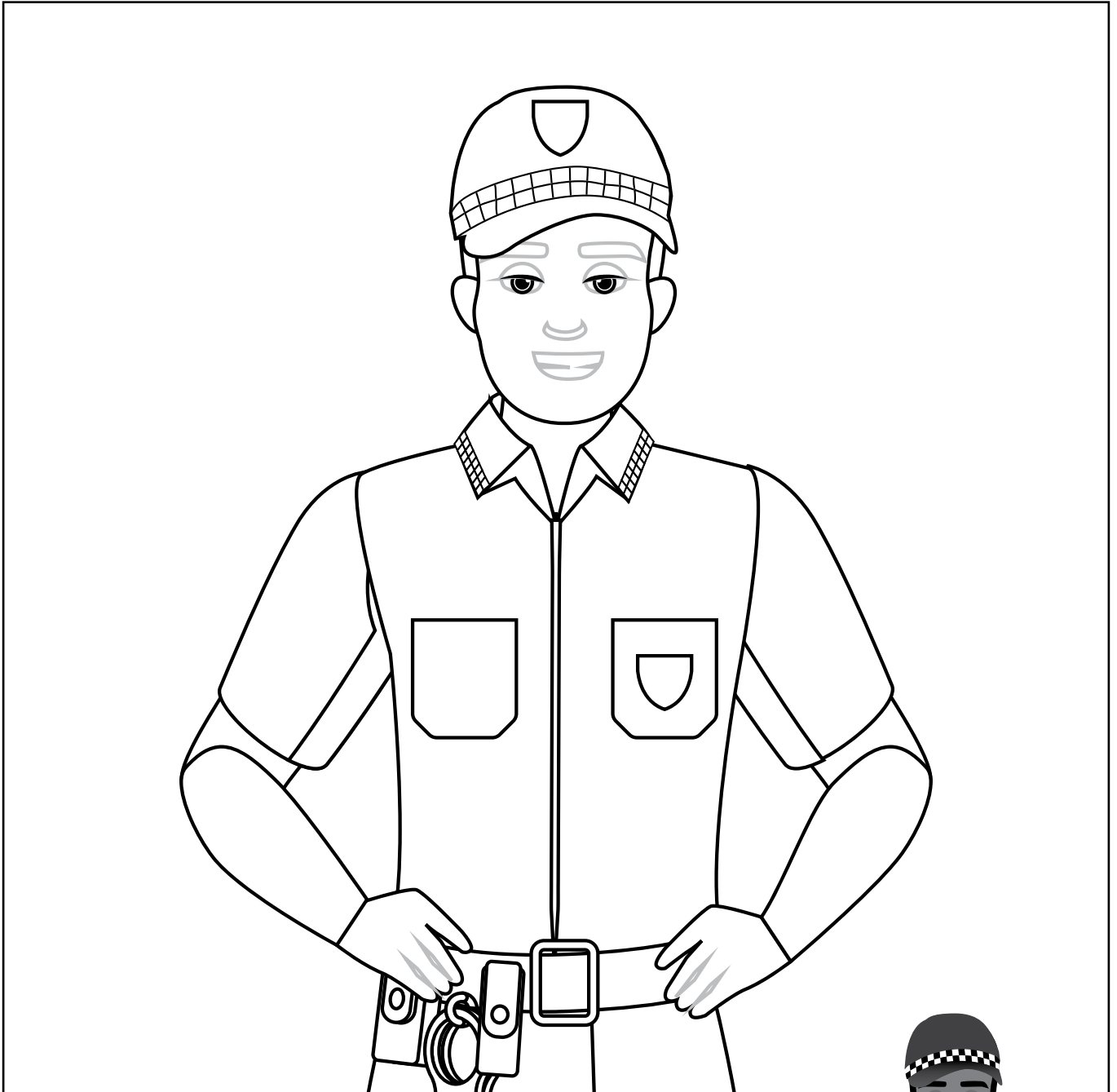
ARE YOU IN CONTROL...

Don't use your year of birth in your username.



TIPS
#10

COLOURING IN DO YOU KNOW THE COLOURS USED IN OUR UNIFORMS?



ARE YOU IN CONTROL...

Never share your passphrases.

HERE ARE SOME TEXT/SMS SCAM EXAMPLES

Show your mum, dad, grandparents, sisters, brothers, uncles, aunts and kids so they know what to be careful of.

Remember... never click on the link.

Your parcel is stored in our depot as we could not deliver successfully. For reschedule purpose, tap <https://s.id/-1aL>

Hey Mum it's me. I got a new number, you can delete the old one



Here -n8- comes your package! <http://reef4perfumes.com/b/sg/?4HV.ty&rCz-U>

FROM COMMBANK

Your action is required - continue to <https://commbank.auth.mob/.netbank/>. & follow the prompts

[Centrelink] Your special benefits are ready for you to claim! Visit <https://centre.to> to get the benefits you deserve.

Notice from the post office: we were unable to deliver your package (and what to do next) concreteriversideca.com/z-ec/?XOlz0v3-cS-G9d8

The account has been deactivated, please update the information in time and reactivate it so as not to affect normal travel. s.id/-1cQf

TRACKING: PARCEL

Delivery had been stopped, please update your address and freight; <https://twss.top>

Authorisation is required to complete delivery. startracker-auspst.com

Hello dear, I am Lisa from LinkdIn, and our recommend a part-time job for you, with salary of \$70~\$150! per hour. Easy work, you come work for 1-2hours each time. To apply reply "YES" or "Interested".

Me ssa g e for y ou: annietiville.com/hya/?h-2JXg LZ3dD-H74g je

ARE YOU IN CONTROL...

Don't trust messages with links.

SPOT THE DIFFERENCE AND COLOUR IN

Spot 5 differences and colour in our uniforms.



ARE YOU IN CONTROL...

Use anti-virus software on your device.



TYPES OF SCAMS TO BE AWARE OF

Phishing:

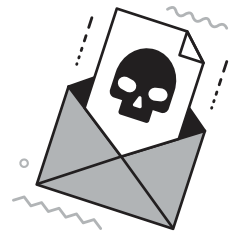
A scammer contacts you out of the blue via email, phone, social media or text message pretending to be from a legitimate business such as a bank, phone or internet service provider.

Usually by emails that 'fish' for you to click on a link and put in your username and passphrase so they can obtain your personal information.



Fake Surveys:

Scammers offer prizes or rewards such as gift cards to well-known retailers in return for completing an online survey. The survey requires you to answer a range of questions including disclosure of important identification or banking details. The more information they have about you the easier it is to rip you off.



Job and Employment:

These scams involve offers to work from home or set up and invest in a 'business opportunity'



Financial Fraud:

If you've sent money or personal banking information to a scammer, contact your bank or credit union immediately.

Report scams to ReportCyber:

www.cyber.gov.au/acsc/report

ARE YOU IN CONTROL...

Perform regular software updates.



PARENTS AND GUARDIANS

Suggestions to help protect your child on the internet



Maintain direct and open communication with your child



Where possible keep all internet-capable devices in common family areas



Know how to disable location services on your child's smart device



Check privacy settings on your child's social media accounts



Be aware of the social media sites on your child's device



Check your child's online profiles and ensure the content is appropriate



Consider password protected settings for installation of age appropriate applications on smart devices and computers



Consider installing filtering and/or blocking software on computers



Know how to save copies of your child's instant messaging chat logs



Monitor your child's phone plans and credit for unusual activity



Consider what device you provide your child



Children should be able to tell you the name of their online friends



Ensure you have access to your child's accounts in order to monitor them



Consider appropriate phone and data plans for your child



Consider syncing smart devices to family account



