

DIGITAL GUARDIAN

▶ ▶ ▶ PLAYBOOK



**EMPOWERING DIGITAL GUARDIANS
EVERYONE PLAYS A ROLE!**

RESOURCES

▶ ▶ ▶ CYBERSECURITY

4 EASY WAYS to stay safe online

Our online world needs to be protected. There are easy things we can do to ensure our information is safe from those wishing to steal it.

Recognize & report phishing

Most successful online intrusions result from a recipient of a “phishing” message accidentally downloading malware or giving their personal information to a spammer. Do not click or engage with these phishing attempts. Instead, recognize them by their use of alarming language or offers that are too good to be true.

Report the phish and delete phishing messages.

Use strong passwords

Simple passwords can be guessed. **Make passwords at least 16 characters long**, random and unique for each account. Use a password manager, a secure program that maintains and creates passwords. This easy-to-use program will store passwords and fill them in automatically on the web.

Turn on multifactor authentication (MFA)

Use MFA on any site that offers it. MFA provides an extra layer of security in addition to a password when logging into accounts and apps, like a face scan or a code sent by text.

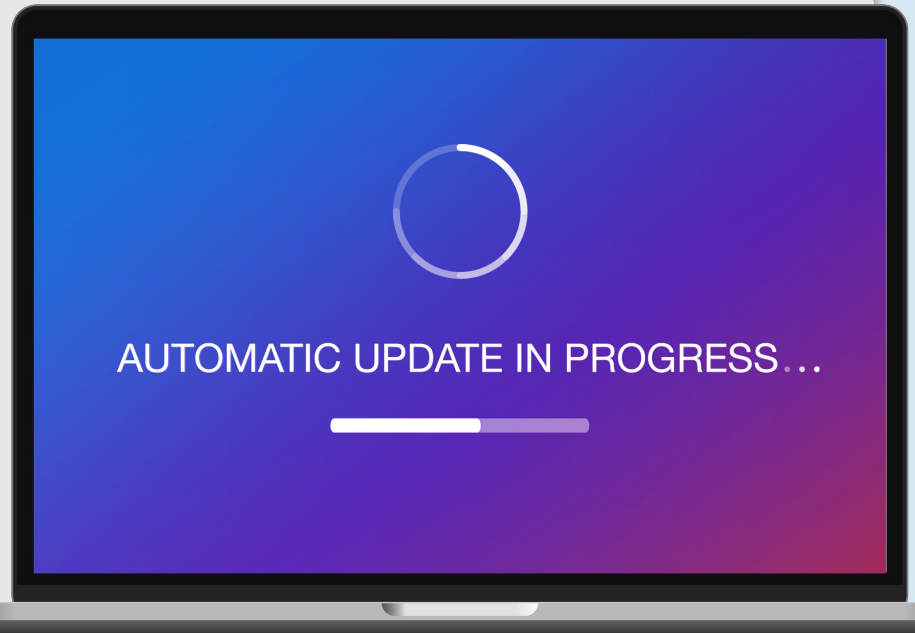
Using MFA will make you much less likely to get hacked.



Update software

When devices, apps or software programs (especially antivirus software) notify us that updates are available, we should install them as soon as possible. Updates close security code bugs to better protect our data.

Turn on automatic updates to make it even easier.



Taking these steps helps
Secure Our World.



We can all help one another stay safer online, so share these tips with a family member or friend!

cisa.gov/SecureOurWorld



Stay **safer** with
**MULTIFACTOR
AUTHENTICATION**
(MFA)

How to turn on MFA

MFA provides extra security for our online accounts and apps. This security could be a code sent via text or email or generated by an app, or biometrics like fingerprints and facial recognition. Using MFA confirms our identities when logging into our accounts.



Follow these easy
steps on each
account



Go to Settings

It may be called Account Settings, Settings & Privacy or similar.

Look for and turn on MFA

It may be called two-factor authentication, two-step verification or similar.

Multifactor Authentication



Confirm

Select how to provide extra login security, such as by entering a code sent via text or email or using facial recognition.

Congratulations!

After setting up MFA, logging in may require completing the MFA security step to prove our identities. It only takes a moment but makes us **significantly safer from malicious hackers!**

Turn on MFA for every online account or app that offers it. Doing so will protect our:



Email



Banking



Social Media



**Online
Purchases**



Identities

Using MFA is one way to
Secure Our World.



We can all help one another
stay safer online, so share these tips
with a family member or friend!

cisa.gov/SecureOurWorld



Weak **PASSWORDS**

are the most common way **online criminals** access accounts

Strengthen Passwords with Three Simple Tips

Using strong passwords with the help of a password manager is one of the easiest ways to protect our accounts and keep our information safe.

1

Make them long

At least 16 characters—longer is stronger!

2

Make them random

Two ways to do this are:

Use a random string of letters (capitals and lower case), numbers and symbols (the strongest!):

cXmnZK65rf*&DaaD

Create a memorable passphrase of 5-7 unrelated words:

HorsPerpleHatRunBayconShoos

→ Get creative with spelling to make it even stronger.

3

Make them unique

Use a different password for each account:

k8dfh8c@Pfv0gB2

LmvF%swVR56s2mW

e246gs%mFs#3tv6

Tip! Use a password manager to remember them.

Let a password manager do the work!

A password manager creates, stores and fills passwords for us automatically. **Then we each only have to remember one strong password**—for the password manager itself. Search trusted sources for “password managers” like Consumer Reports, which offers a selection of highly rated password managers. Read reviews to compare options and find a reputable program for you.

When we choose strong passwords, we make it much harder for someone to steal our:



Data



Money



Identities

Using strong passwords is one way to **Secure Our World.**



We can all help one another stay safer online, so share these tips with a family member or friend!

cisa.gov/SecureOurWorld

OUTSMART online outlaws

Avoid Phishing Scams with Three Simple Tips

Phishing scams are online messages designed to look like they're from a trusted source. We may open what we thought was a safe email, attachment or image only to find ourselves exposed to malware or a scammer looking for our personal data. The good news is we can take precautions to protect our important data. Learn to recognize the signs and report phishing to protect devices and data.

1

Recognize the common signs

- Urgent or emotionally appealing language
- Requests to send personal or financial information
- Unexpected attachments
- Untrusted shortened URLs
- Email addresses that do not match the supposed sender
- Poor writing/misspellings (less common)



2

Resist and report

Report suspicious messages by using the "report spam" feature. If the message is designed to resemble an organization you trust, report the message by alerting the organization using their contact information found on their webpage.

3

Delete

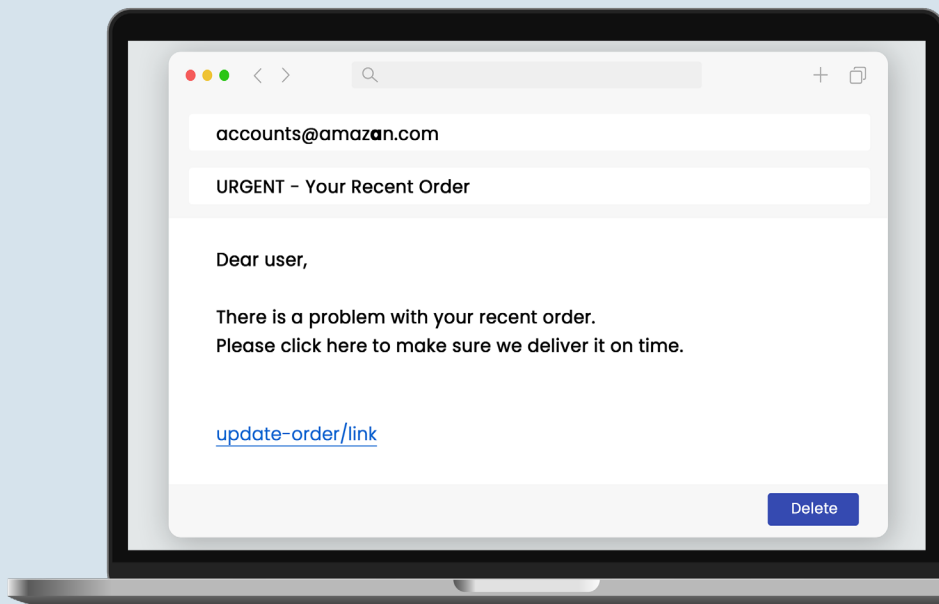
Delete the message. Don't reply or click on any attachment or link, including any "unsubscribe" link. The unsubscribe button could also carry a link used for phishing. **Just delete.**



If a message looks suspicious, it's probably phishing.

But even if there's a possibility it could be real, don't click any link, attachment or call any number. Look up another way to contact a company or person directly:

- Go to a company's website to find their contact information
- Call the individual at a known number and confirm whether they sent the message



Avoiding phishing is one way to
Secure Our World.



We can all help one another
stay safer online, so share these tips
with a family member or friend!

cisa.gov/SecureOurWorld

Install **SOFTWARE UPDATES** to fix **security risks**

Update Software Promptly for Safety

When we see an update alert, many of us tend to hit “Remind me later.” Think twice before delaying a software update! Keeping software up to date is an easy way to stay safer online. **To make it even more convenient, turn on automatic updates!**

Turn on automatic updates

Look in the device’s settings, possibly under Software or Security. Or search the settings for “automatic updates.”

Automatic Updates



Watch for notifications

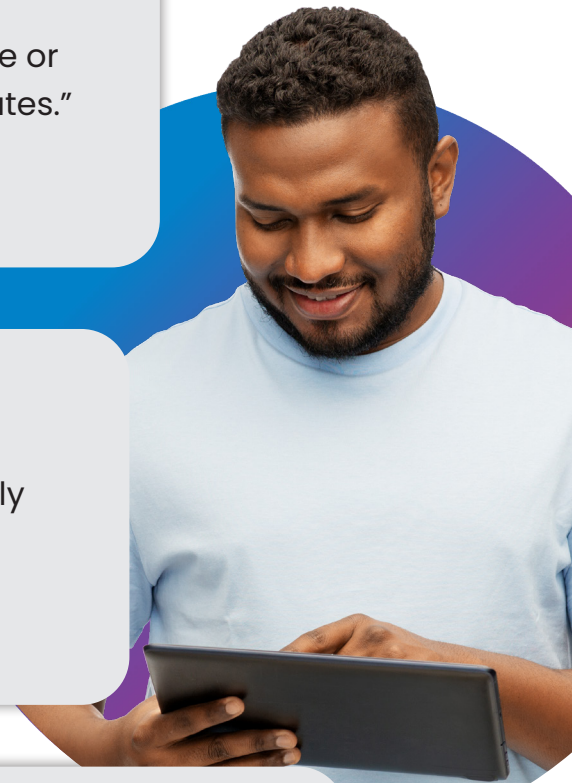


Not every update can be automatic. Devices—mobile phones, tablets and laptops—will usually notify us that we need to run updates. It’s important to install ALL updates, especially for **web browsers and antivirus software.**



Install updates as soon as possible

When notified about software updates, especially critical updates, install them as soon as possible. Online criminals won’t wait so we shouldn’t either!

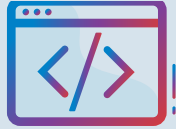


Why it's so important to update promptly

If a criminal gets into a device through a security flaw, they will look for personal information and sensitive data to exploit. Technology providers issue software updates to "patch" security weak spots as quickly as possible.

If we don't install them, they can't protect us!

Software updates can also:



Fix Bugs



**Improve
Performance**



**Install Latest
Features**

Updating software is one way to
Secure Our World.



We can all help one another
stay safer online, so share these tips
with a family member or friend!

cisa.gov/SecureOurWorld

STAY SAFE ONLINE WHEN USING AI

While AI might offer valuable capabilities, always remember to stay proactive and educated about the risks. Here are essential tips to ensure you stay secure while using generative AI.

1. Mind Your Inputs

AI systems learn from user inputs, so refrain from sharing anything you want to keep private, like your workplace's company data or your personal details.

TIP: Avoid sharing sensitive or confidential information with AI models – if you wouldn't post it on social media, don't share it with AI.

2. Be Privacy Aware

Since AI models often scrape data from the web, what you share publicly online may be copied, in whole or in part, by AI tools.

TIP: Think about what you share with a wide audience – would you want an AI to have it?

3. How Hackers Use AI

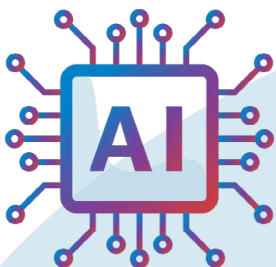
Cybercriminals may use AI to fool you. Public tools can mimic a person's voice or image (this is sometimes called a "deepfake"). Criminals can make a voice call to mimic a trusted person and steal money or to harass people by posting fake or modified images and videos.

TIP: Stay updated on cybersecurity best practices. Criminals using AI as a tool makes it more important that everyone protect themselves using the core 4 behaviors: strong passwords, MFA, software updates, and reporting phishing.

4. AI is a Tool

While AI can assist with tasks, it's important to maintain your expertise and not rely solely on AI-generated content. Prompting isn't the same as creating!

TIP: Treat AI as a helpful tool rather than a replacement for your skills.



Remember: Follow the Core 4

As generative AI increases in popularity, adopting the “Core 4” cybersecurity behaviors is paramount for all of us. Use strong, unique passwords (and a [password manager!](#)), turn on multifactor authentication for all accounts, keep software updated and watch for phishing.



Use strong passwords

[Learn More](#)



Turn on MFA

[Learn More](#)



Keep software updated

[Learn More](#)



Watch for phishing

[Learn More](#)

Taking these steps helps
Secure Our World.



We can all help one another stay safer online, so share these tips with a family member or friend!

cisa.gov/SecureOurWorld

RESOURCES

▷ ▷ ▶ DATA PRIVACY

5 Tips

To Protect Your Privacy Online



- 1** Protect your privacy with passwords.
- 2** Remember that things you post may not be private.
- 3** Respect your friends' privacy.
- 4** Protect your privacy by using a made-up name.
- 5** Ask a parent or guardian for help or permission.

Find out more at: youthprivacy.ca

Request copies: jeunes-youth@priv.gc.ca



Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada



Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario



Commission
d'accès à l'information
du Québec



Office of the Information
& Privacy Commissioner
Nova Scotia



OMBUD NB
N-B
BETH WEIN RESPOND. ÉCOUTER. ÉCLOSER. CLARIFIER.



Manitoba
Ombudsman



OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA



OFFICE OF THE
INFORMATION & PRIVACY COMMISSIONER
for Prince Edward Island



Office of the
Saskatchewan Information
and Privacy Commissioner



Office of the Information and
Privacy Commissioner of Alberta



OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR



OFFICE OF THE
INFORMATION
AND PRIVACY
COMMISSIONER
NORTHWEST TERRITORIES



Yukon
Information
and Privacy
Commissioner

Written by Mark Slutsky • Illustrations by Dan Buller

Cat. No.: IP54-95/2022E-PDF
ISBN: 978-0-660-34435-5

STAYING SAFE ON SOCIAL MEDIA

Social media can help you connect with friends and family, share your interests, or get the latest news. However, sharing personal information online can also put your privacy at risk, and once it's out there, you may not be able to control what happens to it. This could even make you vulnerable to phishing, identity theft or fraud.

STAY SAFE ON SOCIAL MEDIA WITH THESE TIPS ▶



MANAGE YOUR ACCOUNT

- Read the privacy policies
- Choose a strong password for each of your social media accounts
- Customize your privacy settings

CONSIDER THE CONTENT

- Before posting, think through the long-term implications
- Respect the privacy of others
- Review content regularly and delete posts you are no longer comfortable with



AVOID FRAUD, THEFT & SCAMS

- Don't share your location
- Don't open suspicious messages or links
- Don't disclose personal information online unless you are sure you know who you are dealing with

DON'T LEAVE ACCOUNTS OPEN

- Log off when you're done
- Close unused accounts and ask the company to delete your data



Read our complete guidance: priv.gc.ca/socialmedia



Follow us: @PrivacyPrivee



Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

GAMING & YOUR PRIVACY

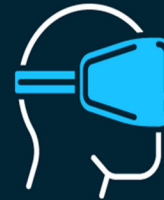
WHAT GAMERS SHOULD KNOW ▶

If you're one of the millions of Canadians who enjoy playing video games, take a moment to understand the potential privacy risks and what you can do to help safeguard your profiles.



**KNOW THE RISKS, SO THAT YOU
CAN UPGRADE YOUR ARMOUR.**

RISKS INCLUDE:



- Your personal information may be shared broadly with third parties
- Gaming and social sites may exchange your personal information
- Someone may attempt online impersonation

USE THIS REAL-TIME STRATEGY TO DEFEND YOUR POSITION:

- Always read privacy policies and terms of service agreements
- Create strong passwords
- Allow multi-factor authentication where possible
- Choose restrictive privacy settings
- Don't share sensitive information like your school, workplace or home address
- Be careful when clicking on links within in-game chats – they could be phishing attempts
- Always download games from a trusted source, such as the official application store of your preferred mobile device



MORE TIPS TO LEVEL UP YOUR PROTECTION:

- Create an email address just for gaming
- Use a nickname



PASSW*ORDS



Choosing the right passwords can help you control your personal information and prevent it from being stolen. If someone gets your password, they may be able to get into your accounts, see your activities and even pretend to be you.



USE PASSPHRASES
OR MAKE PASSWORDS NO LESS
THAN 15 CHARACTERS



AVOID OBVIOUS CHOICES
OR A REFERENCE SOMEONE ELSE
COULD GUESS



USE DIFFERENT PASSWORDS

for different
websites,
accounts
and devices



CHANGE DEFAULT

OR

FACTORY PASSWORDS



Allow multi-factor
authentication
where possible



Don't share
passwords



Use automatic
lock features



Don't use the "remember
password" feature
Automatic logins are risky
if you share a computer



Use a trusted
password manager
secured with a
strong password



If you need to write
down passwords,
keep them offline
in a secure place



Keep Your Students (and Yourself) Safe on Social Media: A Checklist



Best Privacy Practices for Teachers

Social media can be a great tool for modeling digital citizenship. It can also be a vital tool for community building. However, it's important to protect personal information (both yours and your students') everywhere online. Use this list of tips to do a checkup on your social media privacy practices.



Know and Apply Your School's Policies

- ✓ Locate and review the social media guidelines for your school, district, or organization.
- ✓ If such guidelines don't exist, work with administrators and tech specialists to set them up.

- ✓ Share and discuss your social media guidelines with students.



- ✓ Use detailed consent/opt-out forms for parents and caregivers.
- ✓ Keep a private list of students whose parents or caregivers haven't given consent.

Tune Up and Protect Devices and Accounts

- ✓ Strongly consider separate accounts for personal and professional use.
- ✓ Audit the privacy and security settings on your social media accounts.

- ✓ Learn about the social media platforms your students use, even if you're not using them at school.

- ✓ Revise your bio and profile information on your social media accounts.
- ✓ Create a digital file naming convention that doesn't use first or last names.

- ✓ Get photo-editing tools on your devices to easily edit out sensitive information.



- ✓ Regularly review the sharing settings for your digital files and folders.

- ✓ Turn off location data for photos on your mobile devices.
- ✓ Consider archiving or deleting your social media content regularly.

- ✓ Ignore comments and direct or private messages asking for personal information on social media platforms, even from someone you know.

Before You Post: Things to Look Out For

Review posts and media for personally identifiable information before sharing. Things you can't or might not want to share include:

- ✓ Names, addresses, birthdates, phone numbers, and Social Security numbers.
- ✓ Grades, assessments, or any part of a student's academic record.
- ✓ Local points of interest.



- ✓ Students' faces.

- ✓ Handwriting.

- ✓ Names on jerseys, desks, and name tags.

- ✓ School and district names on t-shirts, posters, and buses.

- ✓ Promotional or marketing messages for products that include your students.

Get Families Involved

- ✓ Encourage families to follow your school's social media guidelines when they visit campus, or when they post or comment on school-related social media pages.



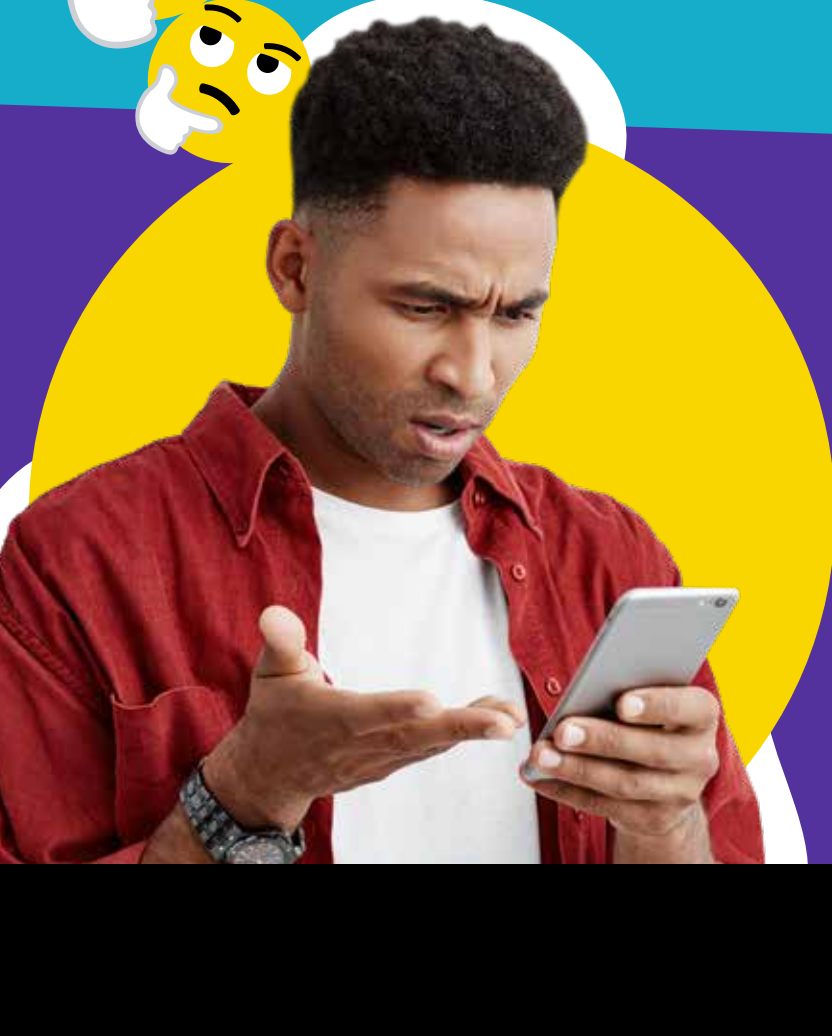
- ✓ Host a family night focused on using social media and devices responsibly at school and home.

Practice in a Safe, Classroom-Only Space

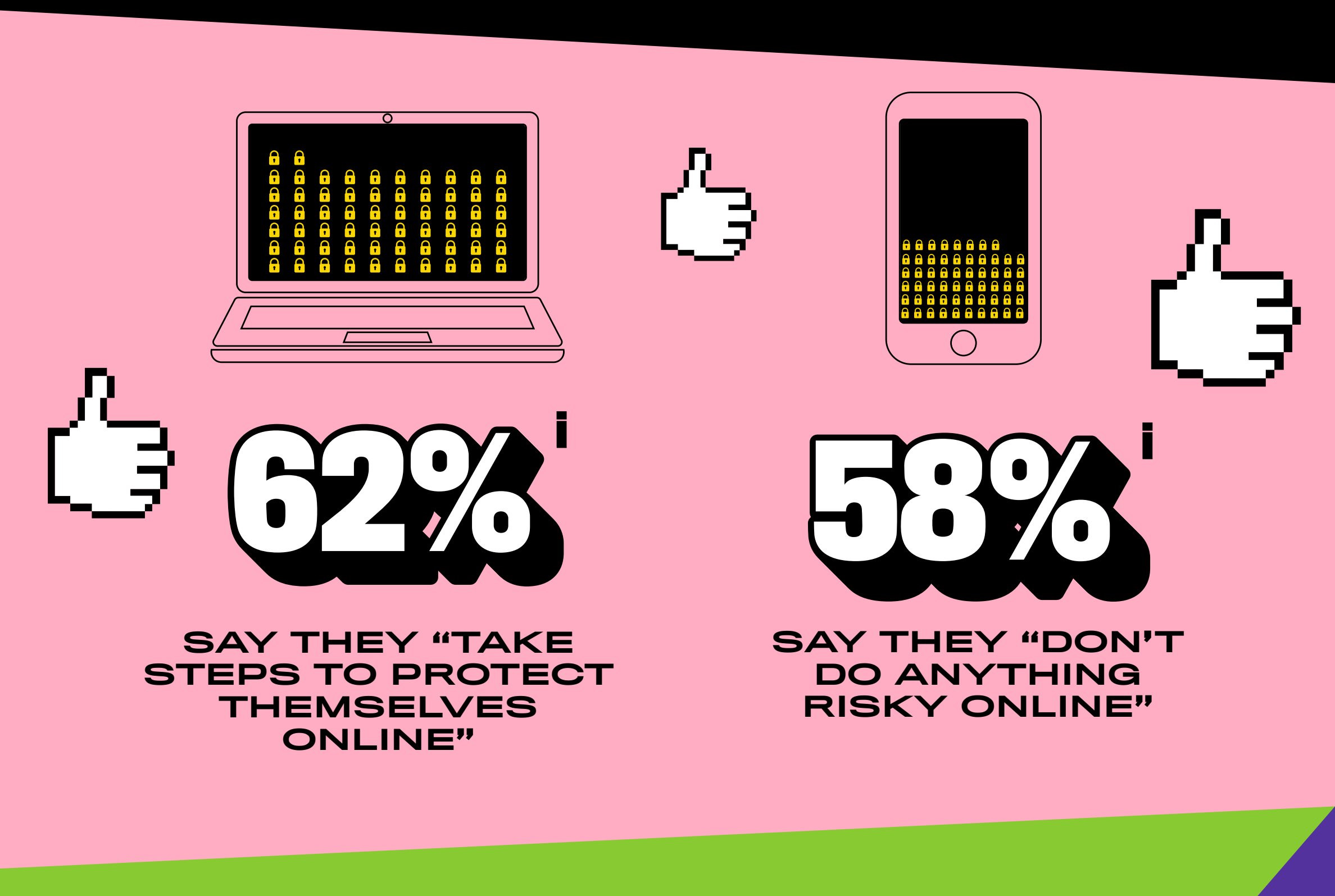
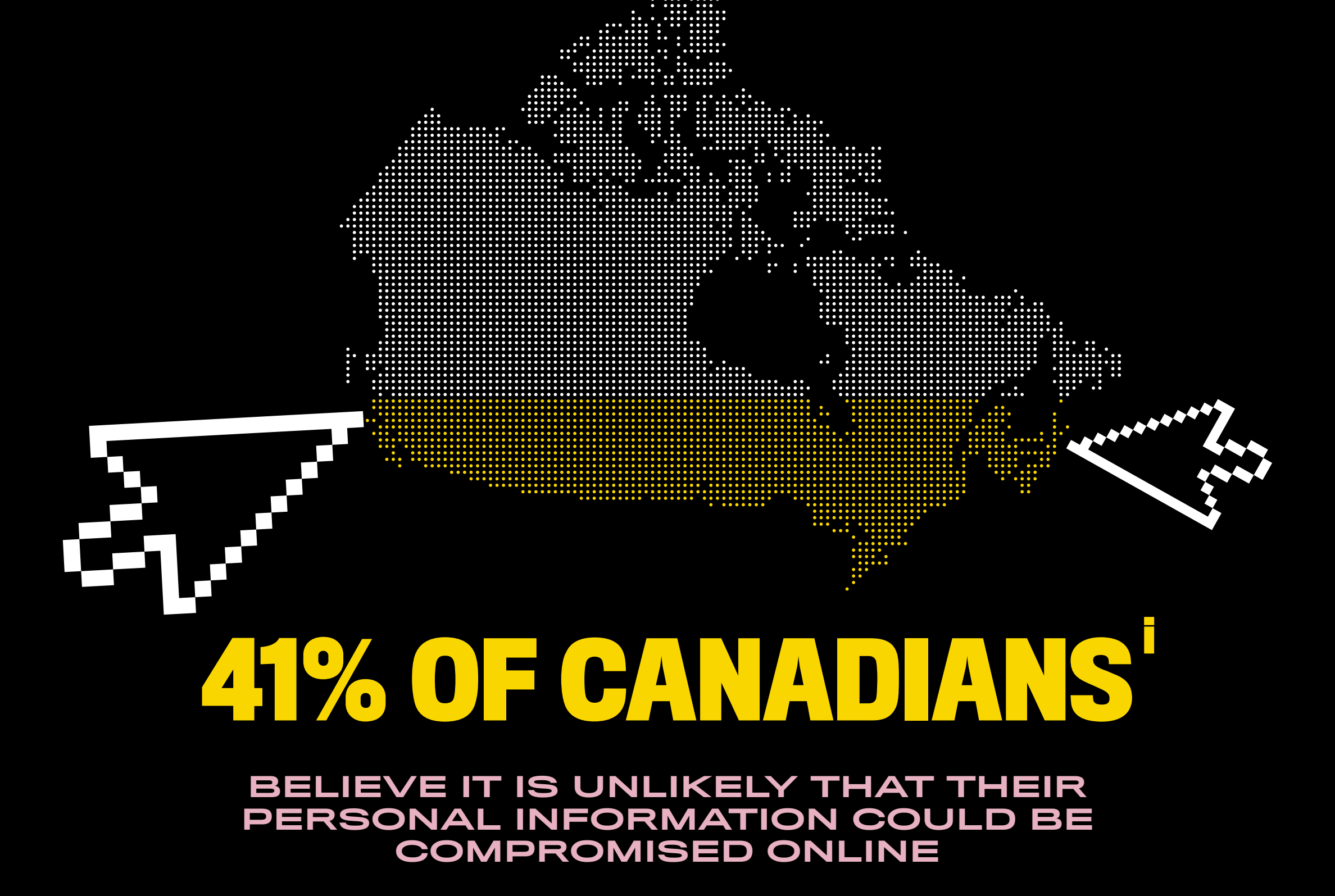
- ✓ Consider using a classroom-only technology, such as a learning management system or messaging app, to share information safely and practice digital citizenship.



WHY DO CYBER SCAMS TRICK US?



It can seem impossible to believe that cyber criminals can get information just by asking for it – but if it were impossible, we wouldn't be here. Cyber threat actors have many scams to get people to give them what they want. Knowing about how they work can help you protect your information online.



BUT MANY CYBER THREAT ACTORS TRY TO TRICK PEOPLE INTO GIVING UP INFORMATION INSTEAD OF TRYING TO ATTACK THEIR DEVICES.



AND THAT'S CALLED SOCIAL ENGINEERING

SO, HOW DOES SOCIAL ENGINEERING WORK?



1 A CYBER CRIMINAL DOES RESEARCH ON

- SEARCH ENGINES
- SOCIAL MEDIA

to learn more about you or your company.

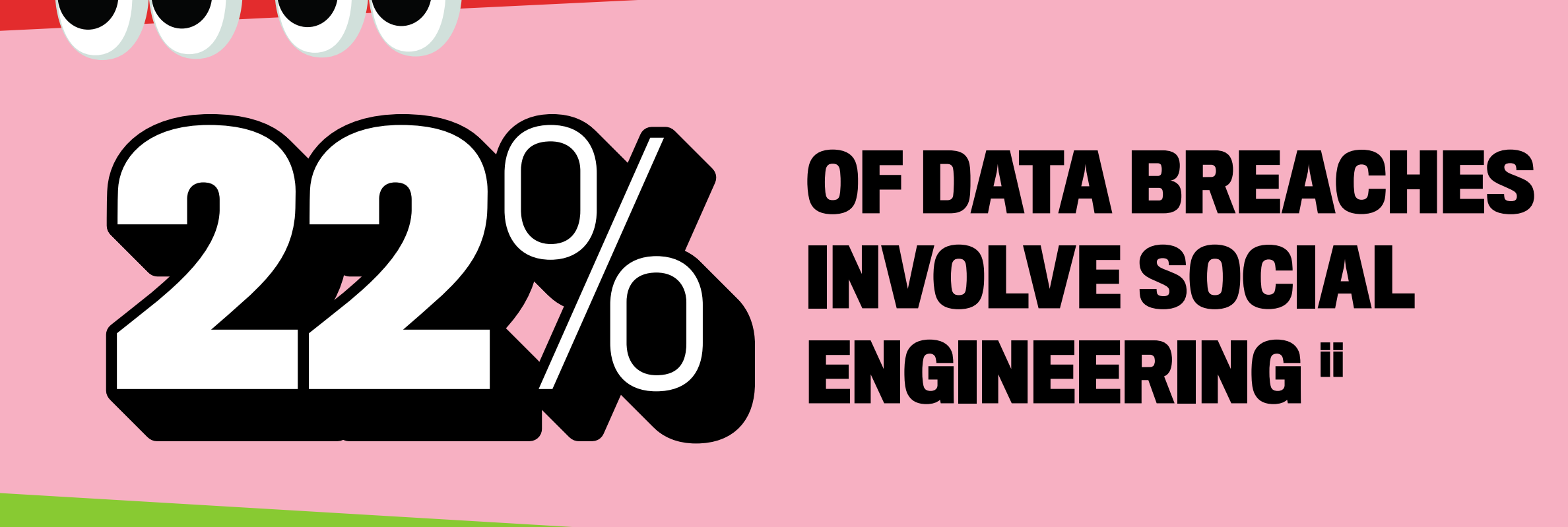
2 THEY SEND YOU A MESSAGE THAT LOOKS LIKE IT'S FROM

- A FRIEND
- YOUR BOSS
- A FAMILIAR COMPANY

or another trusted source.

3 THEY TRICK YOU INTO SENDING SENSITIVE INFORMATION, LIKE

- PASSWORDS
- FINANCIAL DATA
- CREDIT CARD NUMBERS



SOCIAL ENGINEERING IS **TARGETED AND SOPHISTICATED** AND **ANYONE** CAN FALL FOR IT.



(YEAH, EVEN YOU.)

KEEP YOUR INFORMATION SAFE

LIMIT WHAT YOU SHARE ON SOCIAL MEDIA

USE DIFFERENT PASSWORDS FOR EACH ACCOUNT

ALWAYS LOOK OUT FOR SIGNS OF PHISHING

GET MORE TIPS TO PROTECT YOURSELF AND YOUR DEVICES AT [GETCYBERSAFE.CA](https://getcybersafe.ca)

ⁱ Get Cyber Safe Awareness Tracking Survey, 2020
ⁱⁱ Data Breach Investigations Report, Verizon, 2020

TEST YOUR KNOWLEDGE

▶ ▶ ▶ GAMES & TRIVIA

Double Puzzle Answer Key

AOSDRPWS P A S S W O R D

TNRETENI I N T E R N E T

UTDPEA U P D A T E

YRISTCEU S E C U R I T Y

PYRICAV P R I V A C Y

PECTOMUR C O M P U T E R

AEKCHR H A C K E R

EEICVD D E V I C E

IWIF W I F I

RCEBY C Y B E R

IRYFEV V E R I F Y

ELARMWA M A L W A R E

GOILN L O G I N

S T A Y S A F E A N D S E C U R E

O N L I N E

Find the Cyber Terms!

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

Update
Cookies
Encrypt
Email
Internet

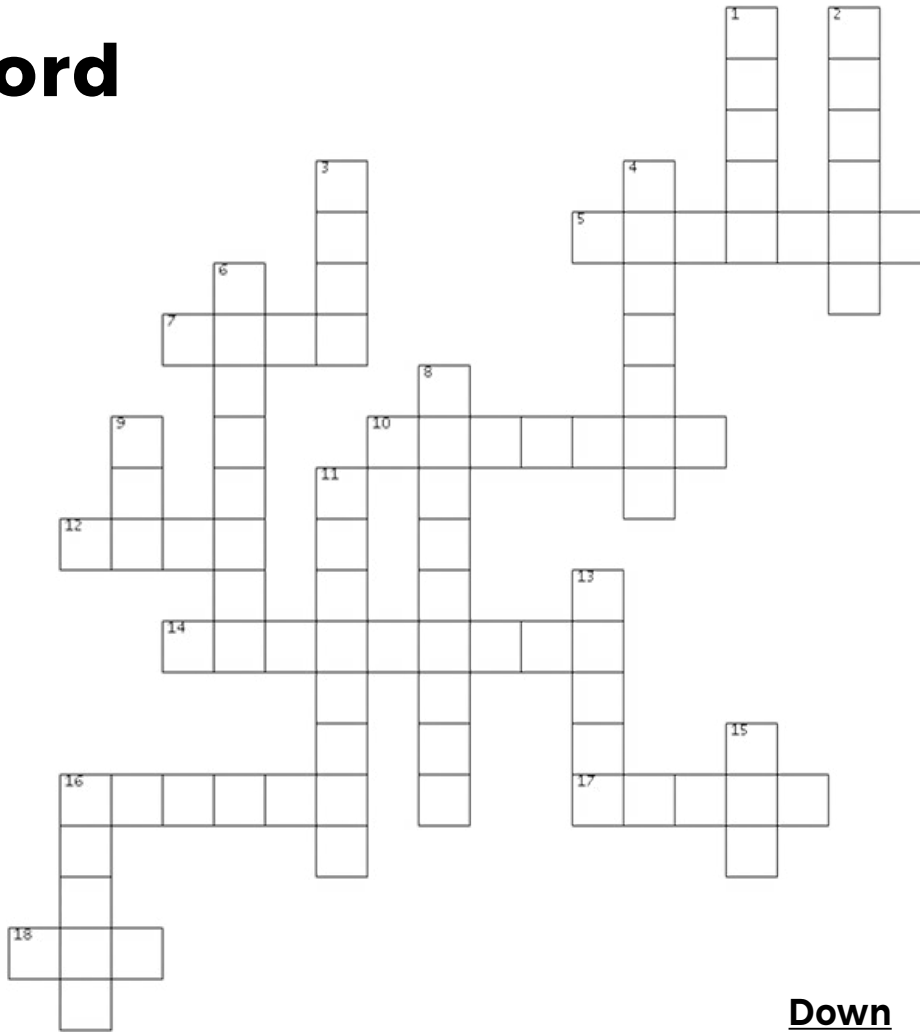
Password
Phish
Malware
Data
Hacker

Virus
Network
Ransomware
Login
Firewall

Word Search Answer Key

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

Crossword



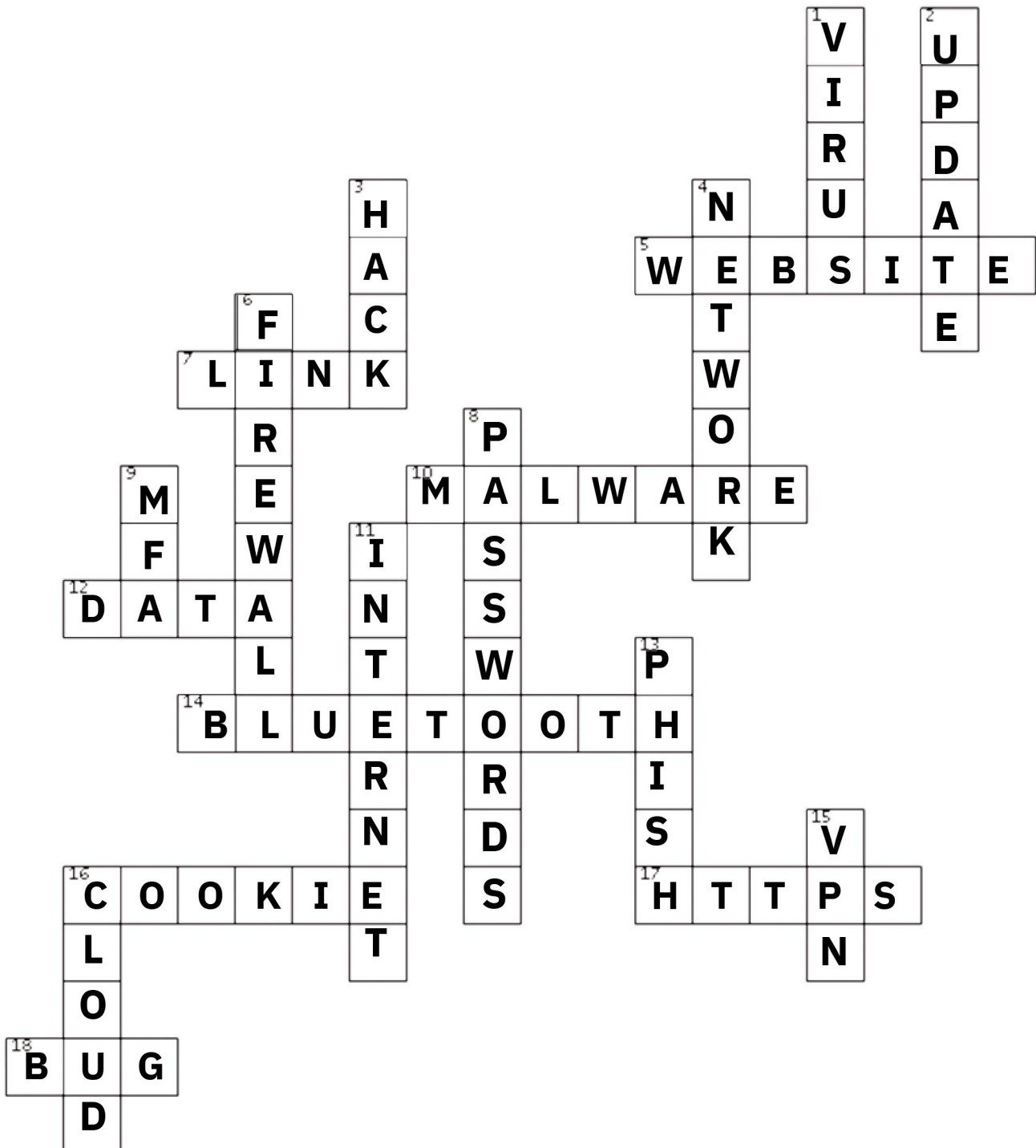
Across

5. Spoofing is when bad actors create a fake _____ and send phish emails to imitate a business.
7. If you receive a suspicious _____ hover over it with your mouse before clicking to make sure it is real!
10. Bad software installed on a computer to damage or harm it. Examples are viruses, Ransomware, Spyware, etcetera.
12. A _____ breach is when a hacker successfully breaks into a system and exposes private information.
14. Wireless short-range connection for devices in the same network. Phones, computers etcetera.
16. A piece of data about your online history that creates a trail of crumbs. Not chocolate chip, though.
17. _____ colon forward slash forward slash before a link website U R L means it is encrypted and secure.
18. A big surprise problem in your computer. Sometimes it is small like an ant or big like a cricket.

Down

1. Malware that infects a computer by corrupting or erasing information and sending it to hackers.
2. Always _____ your devices and software when the newest version is available!
3. When a cybercriminal tries to take your information by sneaking into your computer.
4. When multiple devices are connected together to share information, they are together in a _____.
6. Any tech used to keep bad actors out. It burns the hackers.
8. Always use long and unique _____ for each of your online accounts.
9. This sends an email or text when logging in to make sure it is really you.
11. The online network we use to share information around the world. You use it everyday.
13. When a hacker pretends to be a real person to fool you into clicking on a fake link or file. Usually an email or text message.
15. Private network to make you anonymous on the internet.
16. Global network for servers to share and store information. It doesn't rain from the sky though!






Crossword Answer Key





Wherever there is technology, there needs to be cybersecurity. Make this a collaborative effort by completing this bingo card at your organization. Together, we can build a more secure digital world!

CYBERSECURITY BINGO

<p>Conduct a malware scan on all computers and devices your children or employees use</p>		<p>Discuss with your employees how they can protect both their own and the organization's devices, accounts, and personal information</p>	<p>Investigate what you should do if you are impacted by a data breach</p>	<p>Enable multifactor authentication (MFA) on your accounts</p>
<p>Share links with, or send home CISA tipsheets to, your children's families to encourage safety online</p>	<p>Turn on the auto-lock feature & set a passcode on your devices</p>	<p>Create long, unique, and random passwords for your accounts, update any reused passwords, and look into a password manager</p>	<p>Review the privacy settings on your organization's devices to ensure that it is not sharing its information or location</p>	
<p>Encourage your children to set their social media accounts to private</p>	<p>Talk with your children about online safety</p>		<p>Read about cybersecurity in the news with your children</p>	<p>Contact your regional CISA office to discuss what services they can offer and visit www.CISA.gov/SecureOurWorld for additional resources</p>
	<p>Post CISA's infographic posters in your computer labs or room so your children are reminded of safe practices</p>	<p>Back up important information</p>	<p>Ensure Wi-Fi at your organization is password protected</p>	<p>Delete any apps you no longer use</p>
<p>Present a YouTube video to your children about phishing</p>	<p>Review the privacy settings on your organization's social media accounts</p>	<p>Have your employees watch a CISA webinar and view the animations on actions to take to protect yourself, using www.CISA.gov/SecureOurWorld</p>		<p>Turn on automatic software updates on all devices</p>

NAME: _____



Wherever there is technology, there needs to be cybersecurity. Make this a collaborative effort by completing this bingo card with your parent(s) or another trusted adult. Together, we can build a more secure digital world!

CYBERSECURITY BINGO

Start using a password manager		Hold a family “tech talk” to discuss how each family member can protect their devices, accounts, and personal information	Investigate what you should do if you are impacted by a data breach	Enable multifactor authentication (MFA) on your accounts
Look up cybersecurity tips for using social media safely	Turn on the auto-lock feature & set a passcode on your devices	Research how to create strong passwords and update any reused passwords	Review the privacy settings on your devices	
Set your social media accounts to private	Talk with your parent(s) or legal guardian about whom you are and are not allowed to communicate with online		Read about cybersecurity in the news	Find out what phone apps you have installed that track your location
	Restart your devices to ensure security updates have been fully installed	Back up important information	Learn why public Wi-Fi is not secure and why VPNs are helpful	Discuss with your parent(s) or legal guardian what they are and are not comfortable with you sharing online
Watch a YouTube video about phishing	Tell a friend about this bingo card	Research what you should do if you think you have been phished		Turn on automatic software updates on all devices

Cyber Security Awareness Month 2024 Cybersecurity Q&A

#	QUESTION	ANSWER	ADDITIONAL INFO
1	When was Cybersecurity Awareness Month first celebrated?	October 1, 2004	Initiated by the President and Congress of the United States to raise awareness about cybersecurity.
2	What's the name of the first cyber-attack?	Morris Worm	Created in 1988 by Robert Tappan Morris, it inadvertently infected thousands of computers.
3	When was the first antivirus software created?	1980s	"Elk Cloner" by Rich Skrenta marked the early beginnings of antivirus efforts.
4	What is the most common cyber threat?	Human error	Responsible for 85% of data breaches; occurs due to mistakes by individuals.
5	How much did a ransomware attack cost for businesses on average in 2023?	~\$5m	Ransomware costs vary based on the attack's scale and impact.
6	Does company size matter for a malicious actor wanting to attack?	No, not necessarily	Cybercriminals can target organizations of any size. Vigilance is crucial.
7	What is a phishing attack?	An attempt to trick users into revealing sensitive information	Deceptive emails or websites aiming to steal personal data.
8	Why is it essential to keep software and operating systems up to date?	To patch security vulnerabilities	Regular updates protect against known vulnerabilities.
9	What is two-factor authentication (2FA)?	An additional layer of security beyond passwords	Requires two forms of identification for account access.
10	What is a phishing email?	An email that tricks users into revealing sensitive information	Phishing emails often impersonate legitimate entities and ask for login credentials or personal data.
11	What is a malware?	Malicious software designed to harm or exploit systems	Malware includes viruses, worms, Trojans, ransomware, and spyware.
12	What makes a strong password?	A complex combination of letters, numbers, and symbols	Strong passwords are essential for protecting accounts from unauthorized access.
13	What is a zero-day vulnerability?	A security flaw that is exploited before a fix is available	Zero-day vulnerabilities are exploited by attackers before software vendors can release patches.
14	What is social engineering?	Manipulating people to reveal confidential information	Social engineering tricks individuals into divulging sensitive data or performing actions that compromise security.
15	What is encryption?	Converting data into a secure, unreadable format	Encryption ensures data confidentiality by scrambling information so that only authorized parties can decipher it.
16	What is a brute-force attack?	Repeatedly trying all possible combinations to guess a password	Brute-force attacks aim to crack passwords by systematically testing every possible option.
17	What is multi-factor authentication (MFA)?	Using multiple forms of identification for account access	MFA combines two or more authentication factors (e.g., password, fingerprint, SMS code) to enhance security.
18	What is a security token?	A physical or digital device for authentication	Security tokens generate one-time codes or act as physical keys to verify user identity.
19	What is the principle of least privilege (PoLP)?	Granting users only the minimum necessary access rights	PoLP restricts access to essential functions, reducing the risk of accidental or intentional misuse.



20	What is ransomware?	Malicious software that encrypts files and demands payment for decryption	Ransomware locks users out of their data until a ransom is paid.
22	What is security through obscurity?	Relying on secrecy rather than strong security mechanisms	Security through obscurity is discouraged; robust security should not depend solely on keeping details hidden.
23	What is a security patch?	A software update that fixes security vulnerabilities	Patches address known security issues and should be promptly applied.
24	What is data masking?	Replacing sensitive data with fictional or scrambled values	Data masking protects privacy by ensuring that sensitive information is not exposed in non-production environments.
25	What is end-to-end encryption?	Encrypting data from sender to recipient	
26	<p>What is social engineering in the context of cybersecurity?</p> <p>A) The process of creating software that interacts with users.</p> <p>B) Manipulating people into giving up confidential information.</p> <p>C) Developing systems to manage social media.</p> <p>D) Engineering social networks for better user experience.</p>	B	
32	<p>Which of the following is a common social engineering technique?</p> <p>A) Using a strong firewall.</p> <p>B) Encrypting all data on the network.</p> <p>C) Training employees to recognize phishing emails.</p> <p>D) Installing anti-virus software.</p>	C	
38	<p>What does "phishing" typically involve?</p> <p>A) Hacking into someone's computer remotely.</p> <p>B) Sending fraudulent emails that appear to come from a reputable source.</p> <p>C) Installing malware through USB devices.</p> <p>D) Blocking access to a system unless a ransom is paid.</p>	B	



39	<p>Which of the following can help protect against social engineering attacks?</p> <p>A) Using a strong firewall.</p> <p>B) Encrypting all data on the network.</p> <p>C) Training employees to recognize phishing emails.</p> <p>D) Installing anti-virus software.</p>	C	
40	<p>What is "pretexting" in social engineering?</p> <p>A) The act of creating a fake scenario to obtain sensitive information.</p> <p>B) Sending repeated spam emails to a target.</p> <p>C) Scanning networks for vulnerabilities.</p> <p>D) Infecting a computer with a virus.</p>	A	
41	<p>Tailgating is a physical security breach where an unauthorized person follows an authorized individual into a restricted area.</p>	TRUE	
42	<p>Vishing is a type of social engineering that occurs over the phone.</p>	TRUE	
43	<p>Social engineering attacks always involve technical hacking tools.</p>	FALSE	
44	<p>A social engineer might impersonate a tech support employee to gain access to a company's systems.</p>	TRUE	
45	<p>Baiting involves leaving a malware-infected device in a public place for someone to find and use.</p>	TRUE	
46	<p>What is the main goal of a social engineering attack?</p>	<p>The main goal of a social engineering attack is to manipulate individuals into divulging confidential or sensitive information, or to perform actions that compromise security.</p>	
47	<p>Describe how a social engineer might use "quid pro quo" as a tactic.</p>	<p>In a quid pro quo attack, the social engineer offers something of value (like a free software or tech support) in</p>	



		exchange for information or access, often tricking the victim into compromising their own security.	
48	Why is it important for organizations to conduct regular social engineering awareness training?	Regular training helps employees recognize and respond appropriately to social engineering attempts, reducing the likelihood of successful attacks.	
49	What are some signs that an email might be a phishing attempt?	Signs include unexpected requests for sensitive information, generic greetings, misspelled words or URLs, and a sense of urgency or threat.	
50	How can multi-factor authentication help in reducing the impact of social engineering attacks?	Multi-factor authentication adds an extra layer of security by requiring a second form of verification, making it harder for attackers to gain access even if they obtain a user's credentials.	

Cyber Security Awareness Month 2024 Privacy Q&A

#	QUESTION	ANSWER	ADDITIONAL INFO
1	What does privacy mean?	Broadly speaking, privacy is the right to be let alone, or freedom from interference or intrusion. Information privacy is the right to have some control over how your personal information is collected and used.	https://iapp.org/about/what-is-privacy/
2	Why should I worry about protecting my privacy?	Protecting your privacy means protecting your personal information from misuse and abuse by others.	<p>Identity fraud is an example of a way in which your personal information can be misused if not properly safeguarded. Identity theft refers to the collection or acquisition of someone else's personal information to conduct criminal activities. Identity fraud is the actual use of another person's information in connection with fraud. This includes impersonation and the misuse of debit or credit card information. Fraud committed in your name can take months or years to correct. Meanwhile, the potential consequences can be serious: poor credit ratings; ruined reputations; lost jobs and other opportunities; services denied, and even loss of freedom to travel. Social networks, search engines, and e-commerce sites also collect all sorts of personal information – photos, messages, what you've searched and bought, who you've interacted with. How confident are you that you know what these companies do with that data, why they collect it, and how long they keep it?</p> <p>https://www.ipc.on.ca/en/privacy-individuals/ensuring-your-privacy-is-protected https://www.priv.gc.ca/en/about-the-opc/what-we-do/awareness-campaigns-and-events/privacy-education-for-kids/resources-for-teachers/lesson-plans-for-the-classroom/lesson_04/</p>
3	What three privacy laws protect your personal information at Algonquin College?	FIPPA, PHIPA, PIPEDA	<p>FIPPA for general student information PHIPA for student health information PIPEDA for personal information used for commercial purposes (i.e. shopping at Starbucks)</p>
4	What is a "digital footprint"?	A digital footprint is the trail of data you create while using the Internet. This trail of data comes from the websites you visit, the emails you send and the information you submit or download online. You build your footprint both actively and passively.	<p>Active digital footprint: Data left through intentional actions, such as posting on social media, filling out online forms or agreeing to browser cookies.</p> <p>Passive digital footprints: Data left unintentionally or unknowingly. This data is often collected through monitoring tied to your IP address. Websites and applications may install cookies on devices without disclosure, use</p>



			location tracking or log your activities. https://www.cyber.gc.ca/en/guidance/digital-footprint-itsap00133
5	What are three ways to keep a healthy digital footprint?	Don't overshare, use privacy settings, and only post things you are fine with everyone seeing, including parents, teachers, and potential employers.	It's important to think before you post something. Everything in your profile – comments, photos and yes, even vampire quizzes – could possibly be seen by thousands of people and can be difficult to erase. It's a good idea to think about how ALL the information you are posting can help others form an impression of you, your personality and how you behave in real life. If you're not sure about posting something, don't. https://services.priv.gc.ca/quiz/en/youth
6	When you post something online, can you just delete it without it reappearing?	No	Once you have shared something online, expect that you have lost some control over the information. Someone can always take a screen shot of your content and share it without your knowledge or consent, including content that could be harmful or embarrassing to you in the future.
7	If your social media account is set to private so only your friends can see, is your account actually private?	No	While you attain some level of protection by setting your account to private, this isn't completely foolproof. Your data is still being stored online, where it faces the risk of being sold to third parties. Even when your account is set to private, some advertisers can still access location data, basic profile information and status updates. Before posting information or images on social networking sites, review your default privacy settings and set your preferences so that information is shared only with those you intend to share with. Choose the highest and most restrictive settings available. Also remember that regardless of the audience you chose for your posts, the app is still collecting everything you post. https://ovic.vic.gov.au/privacy/privacy-awareness-week/privacy-quiz-for-young-people/
8	You just started your first year at Algonquin College and you're busy making friends. You've received follower and friend requests from people you don't really know. Do you accept?	No	Many of us have social media "friends" that we would more likely consider acquaintances in real life. Go over your contact list frequently, and restrict access to contacts who are no longer in your 'inner circle.' While you can always delete contacts, it's best to avoid going through that trouble in the first place by being careful when accepting a new request. Only give your real friends access to content that you consider private – someone you don't really know doesn't need all that information about you anyway! https://services.priv.gc.ca/quiz/en/youth
9	Which of the following is true when collecting personal information?	D	Only the data that is needed to fulfill a defined purpose should be collected. For example, your employer needs your banking information to pay



	<p>A) Data can be collected for any reason</p> <p>B) Every organization has access to personal information</p> <p>C) No consent is needed</p> <p>D) Only data needed should be collected</p>		<p>you, but they don't need to know how much money you have in your account.</p> <p>https://quizlet.com/ca/578912969/privacy-quiz-flash-cards/</p>
10	<p>Which of the following are examples of personal information?</p> <p>A) Your student number</p> <p>B) The fact that you are a student at Algonquin College</p> <p>C) A photo of you at a College event</p> <p>D) A, B, and C</p> <p>E) A and C</p>	D	<p>Any information that is personally identifiable to you is considered personal information.</p>
11	<p>Which of these activities are safe to do while using public Wi-Fi networks?</p> <p>A) Online banking</p> <p>B) Shopping</p> <p>C) Completing your tax return</p> <p>D) All of the above</p> <p>E) None of the above</p>	E	<p>None of the above. Public Wi-Fi hotspots may be set up by criminals hoping to steal user information. These networks can be set up to appear legitimate, so there is always a risk that the public network you are using is not secure. Connecting to any Wi-Fi involves transferring data from your device to the network. Private Wi-Fi servers are encrypted and password protected. This means that the information is a lot more difficult to collect or distribute. Public servers are less protected and may be unencrypted. This makes users vulnerable to malware distribution and data theft. Additionally, public Wi-Fi servers have more digital traffic than private networks. This increases the likelihood of cybercriminals targeting a larger pool of users. As a result, criminals are more inclined to target public networks with their scams and viruses.</p> <p>https://ovic.vic.gov.au/privacy/privacy-awareness-week/privacy-quiz-for-young-people/</p>
12	<p>What information is captured by cookies?</p> <p>A) Your approximate location</p> <p>B) Browsing activities, for example, the websites you've visited</p> <p>C) User preferences, for example, language settings</p>	D	<p>For those who don't know, a cookie is a small text file placed on your web browser when you visit a site that uses cookies. Cookies are commonly used to save information about your visit to the website. Different types of cookies will remember different things. First-party cookies often remember customized settings, such as your location and user preferences, while third-party cookies can supply content like advertising on websites you visit—and may be</p>



	D) All of the above		used by third parties to track your browsing activities. https://ovic.vic.gov.au/privacy/privacy-awareness-week/privacy-quiz-for-young-people/
13	What are the top five scams affecting students?	Fake contests, online shopping, online quizzes, phishing/smishing scams, and job scams	https://www.rbcroyalbank.com/en-ca/my-money-matters/money-academy/cyber-security/understanding-cyber-security/top-cyber-scams-affecting-kids-and-youth/
14	What is social engineering?	Manipulating people to reveal confidential information	Social engineering tricks individuals into divulging sensitive data or performing actions that compromise security through tactics such as creating a false sense of urgency (you must pay this ticket!), or impersonating someone the victim knows. Phishing is an example of social engineering.
15	What percentage of data breaches in Canada involve social engineering?	22%	https://www.getcybersafe.gc.ca/en/resources/social-engineering-how-cyber-scams-trick-us