

LESSON PLAN

SHIELDS UP FOR CYBER SAFETY

This lesson is part of *USE, UNDERSTAND & ENGAGE: A Digital Media Literacy Framework for Canadian Schools*: <http://mediasmarts.ca/teacher-resources/digital-literacy-framework>.



LEVEL: Grade 7-9

DURATION: 45-60 Minutes

ABOUT THE AUTHOR: Matthew Johnson, Director of Education, MediaSmarts

Disclaimer: CIRA provides financial support to MediaSmarts. This resource has been developed in collaboration between CIRA and MediaSmarts. MediaSmarts does not endorse any commercial entity, product or service.

Overview

In this lesson, students learn the concept of the Dual-Shield Defense for cybersecurity:

1. The Outer Shield (Technical Perimeter Defenses): Automatic, structural blocks that prevent risks from ever reaching a user's account or device. This includes DNS (domain name system) filtering tools such as CIRA Canadian Shield, ad blockers, multi-factor authentication (MFA), and device-level Stolen Device or Theft Protection.
2. The Inner Shield (Human Cognitive Verification): Active mental habits that allow users to spot, analyze, and neutralize scams that get past the outer shield. This includes detecting psychological triggers

(Urgency, Fear, Authority, Secrecy), applying the "Take Five, Tell Two" rule, and using robust offline verification protocols.

Learning Outcomes

Framework topics: Students will know:

- Privacy and security:
 - Outer Shield Tools: The operational mechanics of CIRA Canadian Shield (DNS-layer filtering), Multi-Factor Authentication (MFA), browser-level ad and script blockers and hardware/software theft protections.
 - Inner Shield Red Flags: The scammer's psychological playbook of emotional triggers—Urgency, Fear/Panic, Fake Authority, and Secrecy/Isolation.
 - Critical Verification Methods: The "Take Five, Tell Two" pause rule, direct URL entry and bookmarking, family code words for voice clones, and the "live hand-wave" test for real-time video deepfakes.

Key concepts: Students will understand that:

- Digital media are networked: Active digital safety is an act of independence that keeps predatory developers, data brokers, and bad actors from manipulating our choices, finances, and data.

- Digital media experiences are shaped by the tools we use: Technical shields are essential for blocking automated noise, but human critical thinking is the ultimate defense when sophisticated threats launder their content through real, trusted services.
- Interactions through digital media have a real impact: Scammers are organized, industrial-scale operators using advanced behavioral psychology to bypass human instincts. Being targeted is a crime of manipulation, and reporting it openly is a sign of strength.

Core competencies: Students will be able to:

- Access: Match and layer Outer Shield settings and Inner Shield habits to neutralize complex, youth-targeted digital risks.
- Use: Make a “Dual-Shield Blueprint” that protects their device and account perimeter while reinforcing their mental verification habits.
- Understand: Deconstruct digital communications to identify the exact point where an Outer Shield was bypassed and where an Inner Shield is required.

Preparation and Materials

Prepare to distribute the handouts *The Dual-Shield Defense* and *Mission Brief: Be Your Household's Chief Security Officer* as well as the assignment sheet *Design Your Personal Dual-Shield Defense*.

If you are conducting the optional live demonstration activity, prepare to project your computer (or a school computer) onto the screen or digital whiteboard and ensure that you are able to access and change the Domain Name System settings.

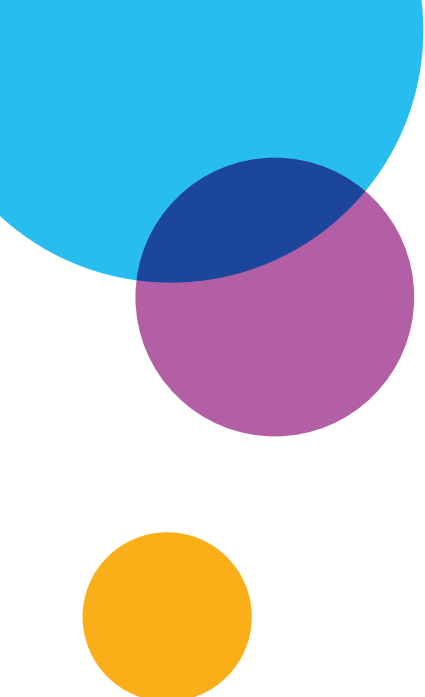
Print and cut out enough copies of the *Threat Analysis Cards* (Scenario cards, Outer Shield Cards, and Inner Shield cards) so that each student group (of 3-4 students) will have one copy of each card.

Procedure

THE GHOST IN THE INBOX

Start by reading students the following text:

Imagine you are looking at one of your digital devices and you get a message from a service you're subscribed to. The sender's address



looks right, and your email provider marks it as 'Safe' with green checkmarks. It says that your account is about to be canceled and gives you a link to follow if you want to stop that.

Take forty-five seconds to write down anything about that message that might make you suspicious.

Now give students 45 seconds to write down any clues they identified.

Go rapidly around the room. Each student should share one clue (e.g., "urgency," "panic," "link to click.")

Once they have shared, tell students that to protect ourselves from scams, malware, and other cybersecurity threats, we need to build two "shields": an Outer Shield of security tools that will block threats from reaching you and keep you from going to dangerous sites, and an Inner Shield of mental habits that will spot scams that don't use malicious files or links.

Tell students:

"The reason you spotted those clues is because you were already looking for deception. Today, we are going to learn how to act on that suspicion by building a Dual-Shield Defense, giving you the all the technical settings and mental habits to keep control of your own data and devices."

THE DUAL-SHIELD DEFENSE

Now tell students that you are going to give them some examples of ways that we keep ourselves safe, and they need to tell you whether each is an "Outer Shield" (a tool that keeps danger away) or an "Inner Shield" (a habit or idea that helps you recognize and deal with a risk.)

Explain that when you give each example, they should cross their arms if it is an example of an Outer Shield, or tap their temples if it's an example of an Inner Shield.

Now read the following prompts. Keep the pace rapid, moving on to the next prompt as soon as the whole class has chosen their actions and you have given them feedback.

- A deadbolt lock on your front door. (Outer Shield: students should cross their arms.)

- Asking “Who is it?” when someone knocks on the door. (Inner Shield: students should tap their temples.)
- Reading the ingredients in a food package to look for anything you’re allergic to. (Inner Shield)
- A tall security fence surrounding a concert venue. (Outer Shield)

Ask students to suggest one more example of an Outer Shield tool and one more example of an Inner Shield habit or idea.

Next, tell students that you are going to give them some examples of ways to protect yourself and your device from cybersecurity risks. As before, tell them to cross their arms if they think it is part of the Outer Shield and to tap their temples if they think it is part of the Inner Shield.

- Using CIRA Canadian Shield on your router, browser or device (Outer Shield: Canadian Shield blocks malware and phishing domains at the domain level, so it will block you from opening or following a link to a dangerous site)
- Pausing for five minutes before reacting to a message (Inner Shield: scammers try to make you scared or upset, so you should always take time to cool down before doing anything)
- Coming up with a family “code word” to verify an emergency call (Inner Shield: this is a way to verify that someone really is who they say they are, and not an AI voice clone or deepfake)
- Installing an ad-blocker on your browser or device (Outer Shield: ad-blockers keep possibly malicious ads from being displayed and limit what data apps and websites can collect)
- Turning multi-factor authentication on (Outer Shield: requiring a second step to access your accounts – like sending a verification message or getting a face or fingerprint scan – means hackers can’t access them if they get your password through a data breach.)

Finally, have students answer the following questions either by doing a thumbs-up if they think the answer is “Yes,” or a thumbs-down if it is “No”:

- *“If I install CIRA Canadian Shield on my phone, do I have to make a decision every time I open a website?”* (Thumbs up: Here you need your inner and outer shields working together. While Canadian Shield will block known threats, making a decision about whether or not you should click is a step you should still always take.

- *“If your parents or guardians get a phone call from someone who sounds like you, can antimalware tools stop that phone call?” (Thumbs down: even on a smartphone, the “Outer Shield” won’t protect you from scams that rely on deception and emotion.)*

OPTIONAL: LIVE DEMONSTRATION

Congratulate students on the sorting activity and tell them that you are going to demonstrate how to do implement one of the “set and forget” tools, CIRA Canadian Shield.

Project your computer or tablet screen onto the classroom board and narrate the following steps:

“Let’s do a 60-second demonstration of how you actually turn one of the Outer Shields on. We’ll use CIRA Canadian Shield as our example. Watch how simple this is:

1. *“First, I open my browser settings and search for ‘Secure DNS’ or ‘Private DNS’.”*
2. *“Next, instead of using the default network provider, I select ‘Custom’ and choose CIRA Canadian Shield, or paste in the CIRA Canadian Shield server address, private.canadianshield.cira.ca.”*
3. *“And done! Now, every time this device requests a webpage, Canadian Shield checks the domain at the core layer to make sure it isn’t a known scam or phishing site.”*

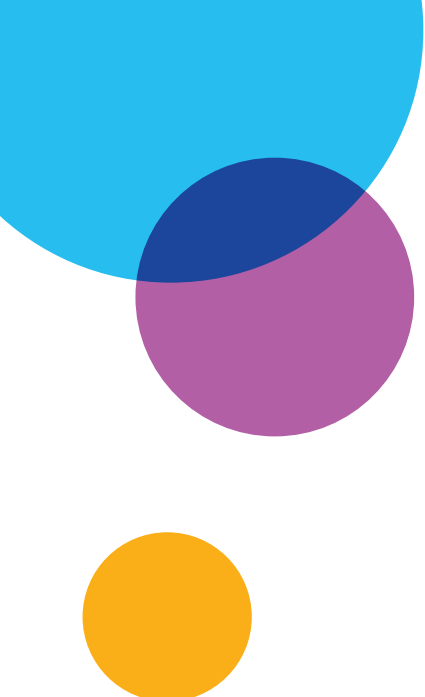
“Now let’s do another ‘Thumbs Up/Thumbs Down. Do I have to make a decision or click ‘Yes’ on every single website I visited?” (Thumbs down.)

No! That is what makes these Outer Shields: you ‘Set and Forget’ them once, and they run automatically in the background to keep automated noise and dangerous links away from your device.”

THE TWO-SHIELD DEFENSE

Distribute the handout *The Two-Shield Defense* and then read students the following scenario:

A scammer wants to steal your gaming funds. They send a tiny payment (one penny) to your account using the real PayPal platform. In the payment note, they write: ‘URGENT: Pending charge of \$987.90 — follow this link or call immediately to cancel!’.



Ask students to think about how the Outer and Inner Shields would help to protect you, then tell them you are going to “think aloud” through it:

Our Outer Shield looks at the email. Because it came from the real service@paypal.com server, it will land in your inbox instead of your Spam filter. CIRA Canadian Shield will stop us from opening links identified as malicious, but we need our Inner Shield to keep us from calling that number and getting scammed. We spot the red flags Urgency (‘immediately’) and Fear (‘charge of \$987.90’) and then “Take Five, Tell Two.” After we take a break and show the email to two other people, we know not to call the number in the email. We open a new tab, type paypal.com directly, and log in to our account securely, where we see there is no charge.

THREAT ANALYSIS

Setup: Group students into teams of 3-4 and give each group a set of Risk Scenario, Outer Shield Tool, and Inner Shield Action cards.

For each of the four Risk Scenarios, groups must work together to identify:

1. Which Outer Shield Tool will work best to prevent or mitigate the threat at the perimeter.
2. Which Inner Shield Action is the best way to protect them if the threat slips through or targets them directly.

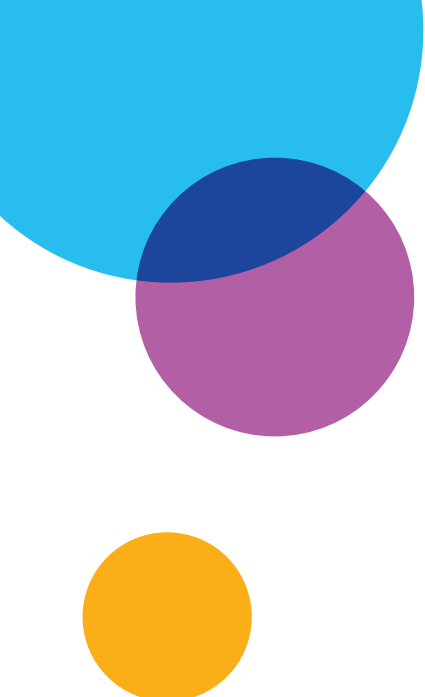
Highlight that while some Shield cards could be helpful for more than one scenario, there is one that is the best fit for each scenario.

Each group should then write a brief, 10-word justification explaining how the two tiers work together to protect them.

When the groups have finished, have the class discuss each scenario and the appropriate “shields”:

RISK SCENARIO CARD	CORRECT OUTER SHIELD CARD	CORRECT INNER SHIELD CARD	CORE DEFENSE CONCEPT
<i>The Subscription Trap</i> While using your browser, you see a social media ad saying you have been selected to win a new phone, but the offer is only open for sixty seconds. If you click the link it will try to download malware onto your device.	<i>CIRA Canadian Shield</i> Blocks malicious malware, phishing, and scam-redirect domains at the DNS layer before a connection is even established.	<i>Identify Red Flags</i> Watch out for the four tactics scammers use to keep you from thinking clearly: urgency, fear, authority and secrecy.	Canadian Shield will stop your devices from even accessing a malicious site. Urgency – like an offer that’s only open for sixty seconds – is one of the four “red flags” of a scam.
<i>The Poison PDF</i> You search for “Free Fortnite skins” and see what looks like a sponsored result. When you click on it, it prompts you to download a “PDF cheat sheet” to unlock your reward. The PDF contains a virus that will infect your device.	<i>Antimalware Tools</i> Device firewalls and antimalware tools protect your device from malware like viruses that you might download in files or attachments.	<i>Don't Expect Something for Nothing</i> Does a deal seem “too good to be true”? If so, it probably is.	Antimalware tools help protect your device from viruses in files, while getting something you want for free definitely seems “too good to be true”!

<i>The Hacked Account</i> You get a message that your social media account has been hacked and you've been locked out of it. The person says they will delete your account if you don't pay them by the end of the day.	<i>Multi-Factor Authentication</i> Enable MFA so login attempts from new devices require a text, fingerprint or app code.	<i>"Take Five, Tell Two"</i> Take five minutes to breathe. Talk to trusted adults to help you find a solution.	Multi-factor authentication makes it much harder for someone to access your accounts, even if they have the password. Taking time to breathe will help you make better choices and trusted adults can help you find a solution.
<i>The Password Leak</i> A database breach at a popular game website leaks millions of user accounts. Since you reuse the same password across your email, Discord, and school accounts, all of them are vulnerable.	<i>Password Manager</i> Use a password manager to generate strong, unique passwords for all your compromised accounts.	<i>Lock & Change</i> If one of your accounts has been breached, don't panic or feel bad about it. Report it to the service, then change your password for that account and for any other accounts that might have been affected.	Password managers prevent cross-account compromises. Reporting a breach and changing your password limits further damage.



Point out to students that in some cases, using the “Inner Shield” might prevent them from needing the “Outer Shield”: if they recognize that the “free Fortnite skins” are “too good to be true,” for example, they won’t download the attachment and won’t need antimalware tools to protect their device from the malware in it.

CHECKING FOR UNDERSTANDING

After the discussion, ask students the following question to test their understanding of how the Outer and Inner Shields work:

“Imagine you have just installed CIRA Canadian Shield on your device. You get a message claiming to be from Canada Post, saying that you have to pay a \$2.50 customs fee to receive a package. There’s a link in the message to pay the fee so you can get your package.

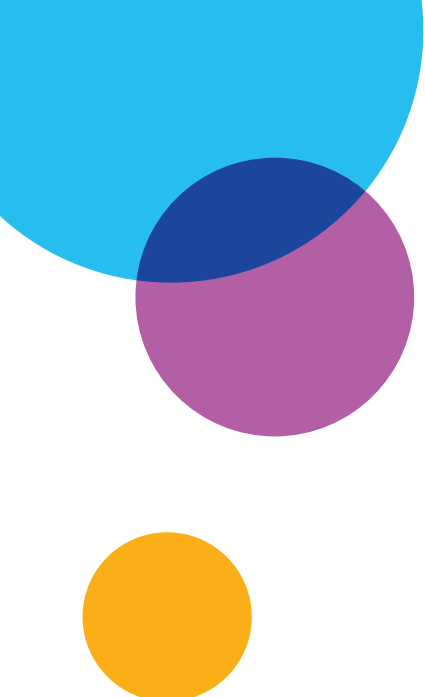
Which of the following is correct?”

- **Option 1:** “If you follow the link, CIRA Canadian Shield will block the connection at the DNS layer if the site is a known malicious scam domain.” (**Correct.**)
- **Option 2:** “Since you have CIRA Canadian Shield installed, a fake text message would be automatically deleted before it ever reached you, so you can click anything safely.” (**Incorrect:** Canadian Shield is a DNS-layer web filter, not an email or text message filter.)
- **Option 3:** “CIRA Canadian Shield will automatically encrypt your payment details as soon as you type them into the custom fee page, keeping your money safe.” (**Incorrect:** A DNS-layer web filter like Canadian Shield will keep you from visiting a malicious web page, but it won’t encrypt the data you send on a legitimate page.)

Have them hold up one finger for Option 1, two fingers for Option 2, or three fingers for Option 3, or have them write their answer on whiteboards and display them.

If three-quarters of the class or more correctly chooses Option 1, go on to the next step.

If fewer than three-quarters of students correctly choose Option 1, use the Door Affordance Analogy to clarify:



“Imagine that your school had a ‘Smart Door’ that would only open for students, teachers and staff of the school.

It wouldn’t stop other students from bothering you and it wouldn’t help if you brought someone in with you, but it would make sure that nobody who wasn’t supposed to be there could open the door.

That’s how a DNS-layer filter works. It blocks the connection to malicious domains, but you might still get malware from downloading a file (like inviting the wrong person in) and you might still get scammed by someone who uses a legitimate payment service.”

YOUR PERSONAL DUAL-SHIELD DEFENSE

Distribute the assignment sheet *Design Your Personal Dual-Shield Defense*.

Have each student fill in the left column (“My Outer Shield Configuration”) and the right column (“My Inner Shield Habits”) with practical actions that draw on what they have learned but are specific to their activities and devices. (For example, if they do not have a mobile device, they should identify Outer Shield tools devices they do have access to, such as laptop computers or gaming consoles; if they play online video games or do online activities such as coding, they should apply Inner Shield tips and habits to the kinds of risks they might encounter in those.)

If you like, you can give students time to research more specific tools and strategies.

Here are some examples of appropriate responses:

1. My Outer Shield Configuration (Set and Forget - 2 Actions):

Choose two technical settings to protect your device perimeter without adding daily frustration:

- *Example A:* Install CIRA Canadian Shield on my phone/browser to block scam domains at the DNS layer.
- *Example B:* Install an ad-blocker like DuckDuckGo on my phone or browser.
- *Example C:* Turn on Multi-Factor Authentication (MFA) on my gaming accounts to block brute-force password breaches.

2. My Inner Shield Habits (Active Mental Verification - 2 Habits):

Choose two cognitive habits to deploy when emotional triggers occur:

- *Example A:* Remind myself to “Take Five, Tell Two” pause if I get a message that my Scratch account has been hacked.
- *Example B:* Use the “Type, Don’t Tap or Call” rule when doing online research—always open a separate browser tab to log in directly instead of clicking notification links or calling provided numbers.
- *Example C:* Set up a secret family password with my grandparents to immediately verify any emergency call or voice message.

Have students rate their confidence in their blueprint from 1 to 5 and write a single sentence explaining why.

Finally, have students trade their blueprints with a partner. Have each partner check if the Outer Shield tools are truly automated (Set-and-Forget) and the Inner actions are mental habits. Next, have each partner borrow one idea from the other’s shield to improve theirs.

REFLECTION

Have students write a brief reflection with the following prompts:

- “I used to think cyber safety was...”
- “Now, I think cyber safety is...”

Right before the end of the class, or if students finish early, ask them to think about the following question:

“As you walk out today: Now that I’ve learned how to protect myself and my devices from cybersecurity threats, what could I do to help my family do the same?”

Have students collect the handout *Mission Brief: Be Your Household’s Chief Security Officer* on their way out. If you wish, you can have students share their thoughts at the beginning of the next class.

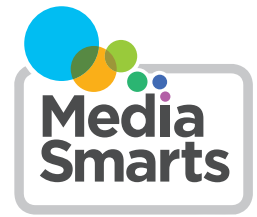
CONSOLIDATION

A day or two after finishing the lesson, ask students to write a two-minute answer to this question:

If a scammer successfully bypasses both shields and I click a bad link or share data, what are my immediate, non-panicked recovery steps?

Take up their answers and highlight the following:

1. Stop and Breathe: Realize I was manipulated by professionals; there is zero shame.
2. Mitigate Immediately: Change my master account passwords, run a full device antivirus scan, and tell a trusted adult.
3. Report the Incident: Block the sender and file a formal report with the Canadian Anti-Fraud Centre to help protect other youth.



SHIELDS UP FOR CYBER SAFETY

THE DUAL-SHIELD DEFENSE

Defending yourself and your devices means making **two shields**: an **outer shield** that stops threats from getting to you and an **inner shield** that helps you recognize risks the outer shield didn't stop.

THE OUTER SHIELD

Automated Perimeter Protection

Blocks malicious connections (CIRA Canadian Shield)

When you try to visit a website, your device asks a "DNS (domain name system) Resolver" to translate a site's address or domain name, like www.cira.ca, into an IP address used to reach that destination. CIRA Canadian Shield (<https://www.cira.ca/en/canadian-shield/>) blocks known malware, phishing, and scam sites at this core layer—preventing a connection to the harmful site from ever being established.

Protects your devices from malware

Use device firewalls and antimalware tools to protect your device from malware like viruses that you might download in files or attachments.

Traps dangerous scripts and ads (Ad-blockers)

Block malicious ad scripts ("malvertising") and tracking cookies used by data brokers and by scammers who want to target you with customized scams based on your interests.

Secures your accounts (strong, unique passwords and Multi Factor Authentication)

Use passwords that are at least 8 characters long, aren't words in the dictionary and don't use easily guessable substitutions (like "1" for "l"). Use different passwords for each account so that if your password for one account is exposed in a data breach, hackers won't be able to access your other accounts. Password managers make it easy to have strong, unique passwords for different accounts.

Require a secondary biometric scan or authenticator code to log in, preventing access even if your password is leaked in a database breach. Enable device-level Stolen Device Protection or Theft Detection Locks so that an extra factor is needed to change critical security settings.

THE INNER SHIELD

Thinking and Feeling Habits

Identifies red flags (Urgency, Fear, Authority, Secrecy)

Scammers use four triggers to override your critical thinking:

- Urgency: messages like "Act in the next 24 hours!" force immediate, impulsive action.
- Fear/Panic: warnings like "Your account will be permanently deleted" or "A courier is coming to pick up cash" provoke a fear response.
- Fake Authority: Posing as trusted organizations (police, banks, Canada Revenue Agency, Netflix, game companies) makes you let down your guard.
- Secrecy/Isolation: Scammers say things like "This is a confidential investigation. Do not tell your parents or friends" to keep you from talking to other people who might help you realize something is a scam.

Deploys verification ("Take Five, Tell Two")

If a message uses any of those four triggers, pause for five minutes to let your adrenaline level drop. Then, tell two different people (a parent, a teacher, a friend). Scammers rely on isolation, so sharing the

SHIELDS UP FOR CYBER SAFETY

story with other people breaks the illusion. Having a “code word” can also help you and your family verify if someone is really talking to you or if it’s a voice clone or deepfake.

Doesn’t expect to get something for nothing

Deals that seem “too good to be true” are another common sign of a scam. There are real deals out there, but you should always double-check to make sure they come from reliable sources.

Uses direct navigation (“Type, Don’t Tap or Call”)

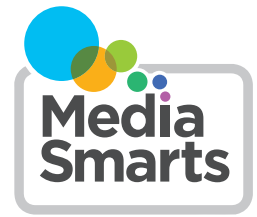
Never follow a link, reply to a message or call a number in any message that uses one of those four triggers. Find the real web address and contact them there.

Responds to security risks

If you learn about a risk to yourself or your devices, fix it. Delete old accounts you don’t use anymore and change your password if one of your accounts has been breached.

Pays it forward

If you or someone you know gets scammed, block the sender and file a report with the Canadian Anti-Fraud Centre at <https://antifraudcentre-centreantifraude.ca/report-signalez-eng.htm> to keep the same thing from happening to other people.



SHIELDS UP FOR CYBER SAFETY

Threat Analysis Cards

.....

SCENARIO CARDS

The Password Leak

A database breach at a popular game website leaks millions of user accounts. Since you reuse the same password across your email, Discord, and school accounts, all of them are vulnerable.

The Hacked Account

You get a message that your social media account has been hacked. The person says they will delete your account if you don't pay them by the end of the day.

The Poison PDF

You search for "Free Fortnite skins" and see what looks like a sponsored result. When you click on it, it prompts you to download a "PDF cheat sheet" to unlock your reward. The PDF contains a virus that will infect your device.

The Subscription Trap

While using your browser, you see a social media ad saying you have been selected to win a new phone, but the offer is only open for sixty seconds. If you click the link it will try to download malware onto your device.

Outer Shield Cards

.....

CIRA Canadian Shield

Blocks known malicious malware, botnet, phishing, and scam-redirect domains at the DNS layer.

Antimalware Tools

Device firewalls and antimalware tools protect your device from malware like viruses that you might download in files or attachments.

Multi-Factor Authentication

Enable MFA so login attempts from new devices require a text, fingerprint or app code.

Password Manager

Use the device's password manager to generate strong, unique passwords for all your compromised accounts.

Inner Shield Cards

.....

Don't Expect Something for Nothing

Does a deal seem “too good to be true”? If so, it probably is.

“Take Five, Tell Two”

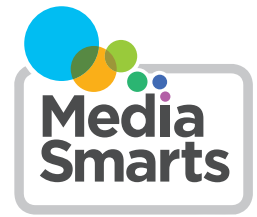
Take five minutes to breathe. Talk to trusted adults to help you find a solution.

Lock & Change

If one of your accounts has been breached, don't panic or feel bad about it. Report it to the service, then change your password for that account and for any other accounts that might have been affected.

Identify Red Flags

Watch out for the four tactics scammers use to keep you from thinking clearly: urgency, fear, authority and secrecy.



SHIELDS UP FOR CYBER SAFETY

Design Your Personal Dual-Shield Defense

YOUR MISSION: BECOME A DIGITAL SAFETY STRATEGIST!

Scammers and hackers use clever tricks to try to sneak onto your devices, steal your accounts, or trick you into giving away secrets. But you are not a target—you are a strategist!

You are going to make a personal Dual-Shield Defense Strategy. These are things you can do right away to make the devices you use and the stuff you do online safer. You will show off your defense by filling in a simple T-Chart.

Step 1: Fill in Your “Outer Shield” (Left Column)

Your Outer Shield is made of automated, technical settings. You set them up once, and they run in the background to block dangers before they ever reach your device.

Write down exactly 2 Outer Shield actions you will take. Make sure they fit the actual devices you use like a phone, a laptop computer, a gaming console, and so on.

Step 2: Fill in Your “Inner Shield” (Right Column)

No technical tool is perfect, and sometimes scams will sneak past your Outer Shield. That is when you activate your Inner Shield—your brain’s detective mode! Other times, using your Inner Shield will mean your Outer Shield doesn’t have to protect you.

Write down exactly 2 Inner Shield habits you will practice. Make sure they match the things you do online like gaming, watching videos, learning about interesting stuff, coding, and so on.

Step 3: Confidence Scale

Rate your confidence in your strategy from 1 to 5 and write a single sentence explaining why you gave that rating.

Step 4: Trading Shields

Trade your blueprint with a partner. Have them check if your Outer Shields are truly automated (Set-and-Forget) and your Inner Shields actions are mental habits. Borrow one tool or habit from their shield to improve yours and add it to either the right or left column.

CHECKLIST: WHAT TO HAND IN

Before you turn in your T-Chart, double-check your work:

[] Do I have exactly 2 specific actions written under my Outer Shield column?

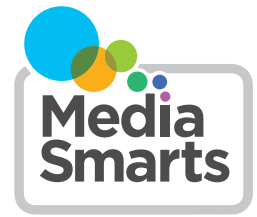
[] Do I have exactly 2 specific habits written under my Inner Shield column?

[] Are my choices customized to my actual devices and the things I like to do online?

[] Have I rated my confidence in my strategy and written a sentence explaining my rating?

[] Have I traded my T-Chart with a partner, given and gotten feedback, and borrowed one of their tools or habits?

MY OUTER SHIELD CONFIGURATION	MY INNER SHIELD HABITS
Set and Forget: 2 Actions <i>Choose two tools or settings to protect your device and yourself without making your life more difficult.</i>	Careful Thinking: 2 Habits <i>Choose two things you will do when anything makes you stressed, upset or suspicious.</i>



SHIELDS UP FOR CYBER SAFETY

MISSION BRIEF: BE YOUR HOUSEHOLD'S CHIEF SECURITY OFFICER

.....

Now that you've learned how to use the Outer and Inner Shields to protect yourself and your devices, your mission is to mentor your family and ensure that everyone stays safe from scammers and cybersecurity threats.

MISSION 1: PROTECTING YOUR PARENTS/GUARDIANS (THE FOUNDATION)

Parents and Guardians often handle the family's most important accounts, like banking and taxes. Ask if they have set up these parts of the Shield:

OUTER SHIELD (SET & FORGET)	INNER SHIELD (MENTAL HABITS)
Install CIRA Canadian Shield: Ask if your parents or guardians have set this up on your home router and on all connected devices. It uses DNS-layer filtering to block connections to malicious sites before they even start.	"Take Five, Tell Two:" Got a message that is worrying or upsetting? Take five minutes to calm down and talk to two people to see whether it might be a scam.
Password Managers: Generates strong, unique passwords so one leak doesn't ruin every account.	"Type, Don't Tap or Call": Never click message links; always type the real website address into your browser.
Stolen Device Protection: Uses biometric scans to lock sensitive settings if a phone is physically lost.	Verify Account Status: If a message claims there is a problem, log in directly to the real site to check.

MISSION 2: COACHING YOUR SIBLINGS (THE GAME PLAN)

Siblings are often targeted through games and social media. Work together with your parents or guardians to help them build a "Sibling Shield" to protect their tablets and consoles.

- Ad-blockers (Outer Shield): These stop "poison" ads and malicious scripts from appearing on websites.
- Antimalware (Outer Shield): This acts as a digital fence, blocking viruses found in "free" downloads or attachments.
- Spotting "Too Good to Be True" (Inner Shield): Coach your siblings to recognize that deals for "free" game skins or cheat sheets are usually tricks to steal data.
- The Golden Rule: Always ask an adult before clicking a "Free" link or downloading a new file.

MISSION 3: SUPPORTING YOUR GRANDPARENTS (THE VERIFICATION EXPERTS)

Grandparents are often targeted by high-pressure scammers using AI and deception. Talk with your parents or guardians about empowering them to be “Inner Shield” experts with these steps:

1. Create a Secret Family Code Word: Choose a specific word to verify voice calls. If someone calls claiming to be a family member in trouble, they must know the code.
2. Identify the Four Triggers: Teach them that scammers use Urgency (Act now!), Fear/Panic (You are in trouble!), Fake Authority (I’m with the government!), and Secrecy/Isolation (Don’t tell anyone!) to stop people from thinking clearly.
3. The “Type, Don’t Tap” Rule Never click links in messages claiming to be from senders like banks, “CRA,” or “Netflix”: always manually type the web address into the browser. You can help them bookmark the correct web addresses of all their banks, streamers, and other services so they don’t have to type them every time.

With these two shields in place, your home is now a fortress of cyber safety!