Digital Smarts

Workshop Script

Financial contribution from

Public Health Agency of Canada
Agence de la santé publique du Canada

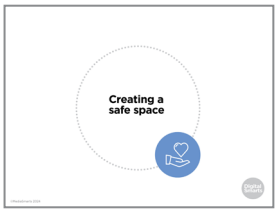
Media Smarts

1. Welcome to our session on online privacy. This workshop is designed to introduce some essential skills for managing your privacy and protecting the security of your digital devices online.

We're going to have some time for questions at the end, but I'd also like to invite you to just raise your hand any time you have a question along the way. *[remote delivery: put your question into the chat]*

2. This workshop is accompanied by a number of support materials, including a practice sheet and video to help you remember the key content.

You can return to these materials at any time, including after the workshop, and you can return to the workshop itself on the MediaSmarts website: https://mediasmarts.ca/resilience-through-digitalsmarts.



3. This workshop touches on some topics that may be upsetting, so before we get started, let's talk about how we can create a safe space here.

We'll let you know what's coming up in each part of this workshop, so you can step away for a few minutes if you'd rather not deal with a particular topic. If you do need to step away, please give me a thumbs-up hand gesture before you leave so I can know you are OK. If you need assistance, *[name of person available for additional support]* is available to support, you.

For remote delivery only: Next, let's make sure you're in a safe place to participate. Are you in a private space where you can potentially share your thoughts and listen without someone you do not trust over-hearing? If not, is there somewhere else you can move to that would allow you more privacy?

If you can, make sure you have something nearby that brings you comfort. We will have scheduled breaks during the workshop, but you should also feel free to step away any time you need to.

4. The focus of this workshop is on introducing some essential skills to manage your online privacy and security. First, we will do a brief survey to help us understand what you know and what you do not know about online privacy and security. Then we will cover the following topics and engage in some exercises to practice these skills:

Protect your privacy online;

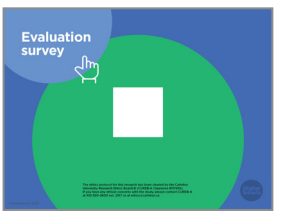
Use privacy settings on social networks;

Make good decisions about sharing things online;

and Fix common things that can go wrong online.

As we go through these topics, we will have two scheduled breaks to allow us to pause and check in. We will end the workshop with another brief survey to help us understand whether this workshop improved your skills in managing your online privacy and security, and wrap up with a simple debrief exercise.

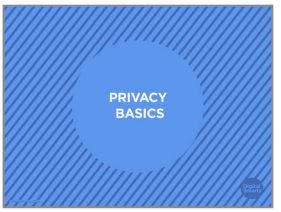
Let's pause for a moment to see if anyone has any questions before we begin.



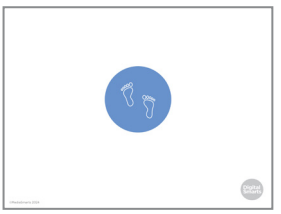
5. There are two opportunities to provide feedback on this program to the team at MediaSmarts who developed this workshop: Now, before we get into the workshop content, and another at the very end. These surveys will help the team at MediaSmarts better understand if the workshop is doing a good job of supporting survivors' digital knowledge, skills, and confidence.

Before we get started with the workshop content, we invite you to take 5 minutes to complete this survey. The MediaSmarts team who developed this workshop will use your responses to guide future updates and to assess the value of this workshop. All your answers will be anonymous. The aim is to evaluate the program, not you, the participants -- it is perfectly fine if you are unsure how to answer certain questions, or don't have the skills being asked about in the survey.

Your participation is completely voluntary. If you're interested in taking the survey, all you need to do is scan the QR code on your phone, or type in the link on your browser to access it. We will pause until everyone who is interested has completed the survey; please take your time.



6. Let's start with some basics about privacy on the internet.



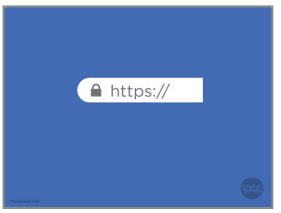
7. The internet is a network. Everything on it is connected to everything else. Any time you visit a website or use an app on your tablet or smartphone, you leave tracks – digital footprints.

Sometimes we know when we leave these footprints, like when you share a photo. Sometimes you may not know what a website or app knows about you after you use it.

Either way, using the internet is like stepping in wet cement. The footprints you leave there last forever.

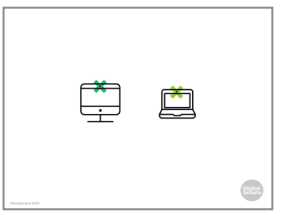
8. Because of that, it's important to be careful what you share online.

For example, you should never post things like credit card numbers, bank information, or passwords anywhere online except when you're on your bank's website or a shopping site you trust and that you know is secure.



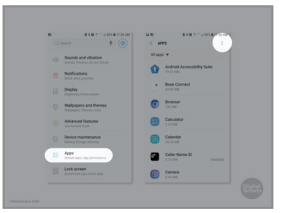
9. You'll know a site is secure because the web address ends in https (not just http) and there's a picture of a padlock in the address bar. That means that whatever you send to it – like credit card information - is *encrypted:* nobody else can intercept and read it.

That doesn't necessarily mean that the site itself is trustworthy, though. We look at how to find that out in the *Introducing Online Basics* workshop.

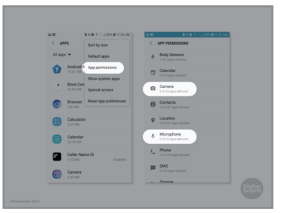


10. You can also cover the cameras on laptops and other devices when you're not using them. That way if you forget to end a call, or if somebody has put spyware on your device, they can't see anything with the camera. You can do this with a sticky note, a sticker or something similar that's easy to take off when you want to use the camera.

11. Turning off the microphone on your devices is a bit trickier, but it's a good habit too.

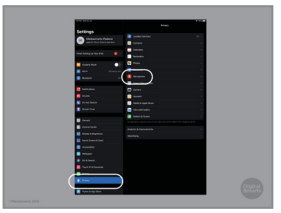


12. Let's go through how to turn off your microphone. On Android devices, tap Settings (the gear icon) and then Apps. Tap the three dots at the top right of the screen,

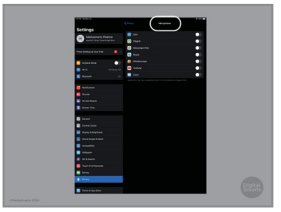


13. In the window that pops up, tap App Permissions. Now you can tap Microphone or Camera.

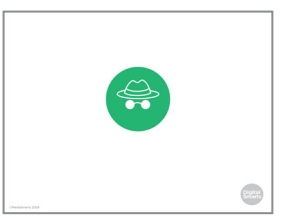
14. Now you can see any apps that have access to the microphone or the camera. Slide them to the left to turn them off – you can always turn them back on later.



15. On an iPhone or iPad, go to settings and tap Privacy.



16. Next, tap Microphone and slide everything to the left. You can do the same with the camera.



17. You can control how much your computer remembers by using Incognito or Private Browsing mode.

Using this keeps your browser from recording which sites you visit. It also won't remember any account information or passwords that you enter.

Just remember that it doesn't usually stop the websites or your internet service provider from recording what you do there.

18. That matters because websites and advertisers use what they know to make a profile of you. They use that profile to decide what advertisements to show you, but it may also be used to decide everything from how much you pay for things to whether or not you can get insurance.

19. There are ways that you can limit how much apps and websites, and the companies that own them, know about you.

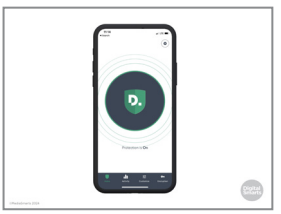
The best ways to do this are to use a browser that's designed to give you more privacy, like Firefox or Brave, and to use extensions that protect your privacy.

Extensions are little programs that work with your browser.

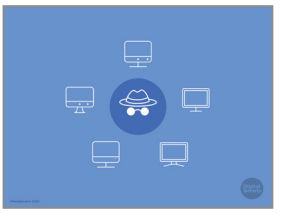
To find extensions on Firefox, click on Add-Ons and Themes and then search for the extension you want.

On Chrome and Edge, click on Extensions; on Safari, click Safari Extensions.

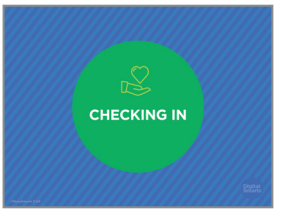
Privacy Badger, Ghostery and Disconnect are all extensions that will block most websites from tracking you online.



20. There is also a Disconnect app you can get for iOS or Android devices.

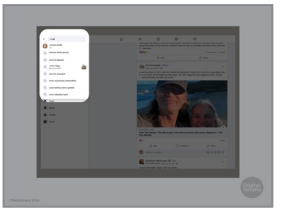


21. If you're using a computer that isn't yours, like a friend's or a public computer at the library, always use private browsing if you can. If you can't, make sure to click "No" any time the browser asks if it should remember your account or password for next time.



22. Before we go on, let's pause for a moment to see if anybody wants to take a break or needs any support.

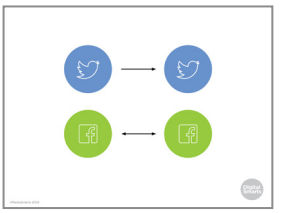
23. Now that we've covered the basics, let's talk about keeping yourself private when you're using social networks.



24. You may already be using a social network like Facebook, or you might just be thinking about starting to use them.

Once you've signed up, you can look for the names of people you know and connect with them.

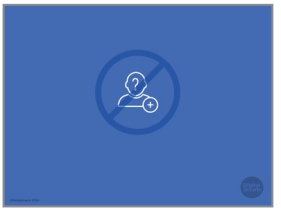
Once you've started to make connections, a lot of social networks also suggest people they think you might know or might want to connect with.



25. There are lots of different social networks, but when it comes to privacy there are really only two kinds of social networks we need to be aware of.

Some social networks are open. Anything you post on an open network can be seen by anyone who chooses to "follow" you, and you don't automatically see what they post. Twitter (now X), YouTube, and TikTok are all open social networks.

On closed social networks, two people have to decide to "friend" one another. Only your friends can see what you post, and you see what they post. Facebook and Instagram are examples of closed networks.



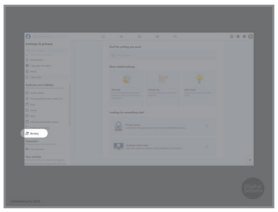
26. You have to think carefully about who you accept as a friend on a closed network, because they see everything you post and can share it with their own friends – who may not be the same as yours.

Don't accept friend requests from people you don't know or don't trust.

We'll look at how you can control which friends see which posts in a few minutes.

27. If you Friend someone and later change your mind, you can Unfriend them. That means they won't see your posts anymore and you won't see theirs.

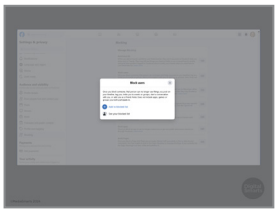
To Unfriend someone, go to their timeline, click on Friends and then click Unfriend.



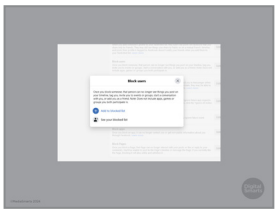
28. If you want to totally cut off contact from someone you can Block them.

If you Block someone, they can't send you a new Friend request, can't see anything on your profile and can't send you messages on that network.

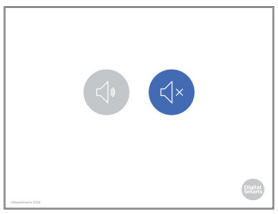
To block someone, go to your profile and click Settings and Privacy



29. Click "Privacy," then "Blocking" –

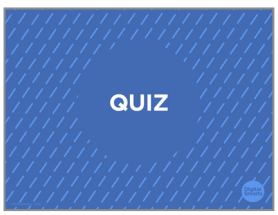


30. Click "Edit" next to "Block Users" and then type the name of the person you want to block.



31. If you want a break from someone but don't want to block or unfriend them, most social networks let you "mute" people. This means that you're still connected but you don't see their posts until you unmute them.

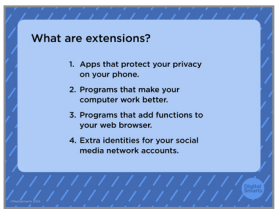
People aren't told that you've muted them, so your friend who's posting pictures from their beach vacation won't be offended that you muted them while they were away.



32. Let's do a quick quiz to review what we've learned so far.

33. Which of these web addresses means that nobody can spy on information you send to it?

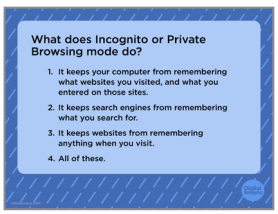
34. Remember there are two things to watch for: the padlock symbol and a Web address then starts with https, not just http.



35. What are extensions?

Are they apps that protect your privacy on your phone, programs that make your computer work better, programs that add functions to your web browser, or extra identities for your social network accounts?

36. Extensions – which are sometimes also called add-ons or plug-ins – add functions to your web browser. Extensions like Privacy Badger are powerful tools to protect your privacy online.



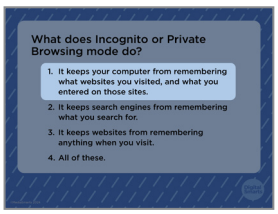
37. What does “Incognito” or “Private Browsing” mode do?

Does it keep your computer from remembering what websites you visited, and what you entered on those sites?

Does it keep search engines from remembering what you search for?

Does it keep websites from remembering anything when you visit?

Or does it do all of those?



38. Incognito or Private Browsing mode *only* stops your own computer from remembering what websites you visited, and what you entered on those sites.

If you don’t want search engines to remember what you searched for, you have to choose a search engine that doesn’t track you like DuckDuckGo.

39. How *can* you stop websites from collecting information about you when you use them?

Is it by only using paid versions of those sites? By entering fake information? By using anti-malware software, like Windows Defender? Or by using browser extensions like Privacy Badger?

40. Browser extensions like Privacy Badger are the best way to stop websites from collecting information.

41. Now let's try putting that into practice.

Take a few minutes to check out a social network you've heard of but don't know much about. It could be Instagram, Whatsapp, TikTok – it's up to you.

Do a search for it on Wikipedia.org or Commonsensemedia.org. See if you can find out these things about it:

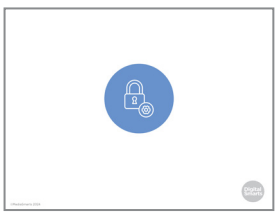
Is it open or closed?

Does it have a safety centre?

Do its privacy tools let you control who can see what you post, who can contact you, and who can tag you?

Are its terms of service readable? If not, is there a readable version of them somewhere online? Check out the website tosdr.org to see if they have a summary.

What answers did you get? How easy was it to find the information? What impression of the social network did you end up with?

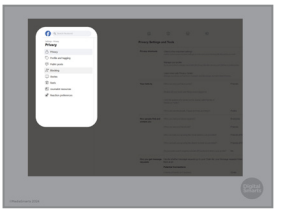


42. So far we've talked about the basic ways that social networks affect your online privacy.

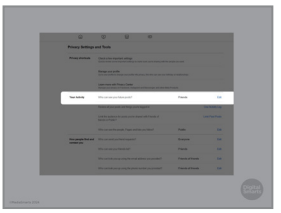
Almost all networks also have privacy settings that give you a bit more control over who sees what you post.

You can change the default privacy settings, so that all of your posts are seen by more or fewer people than usual.

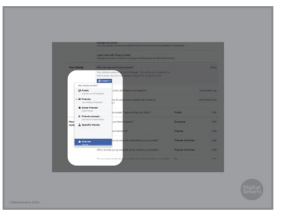
On a lot of networks, you can also choose different privacy settings for each post, so you can make some totally public or decide that some of your friends will see it but not others.



43. To change your settings on Facebook, click Settings and then click on Privacy on the left menu.



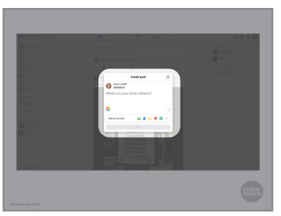
44. Then look for “Who can see your future posts?” under “Your activity”



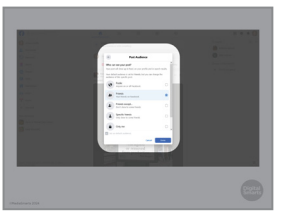
45. Now you can set it so that people who aren’t your friends see your posts – not a good idea because anyone can see them.

You can also leave some friends out, or set it so that just some of your friends see your posts, or so that only you can see them.

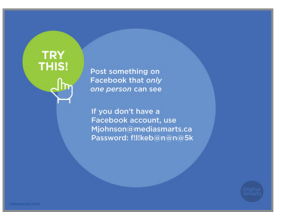
This can be a good choice if you find you often post things you wish you hadn’t. Set your default to “Only Me,” then a few hours later you can go back and decide if you want your friends to see this after all.



46. You can do this with each post too.

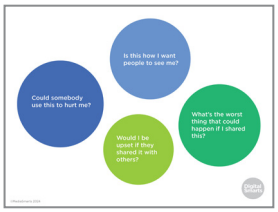


47. So if you want you can let all of your friends see most of what you post, but share some posts with just a few of them – or even just one person.



48. Now let’s see how well you can use Facebook’s privacy settings. Try to post something on Facebook that only one person can see.

If you don’t have a Facebook account, you can log into this one we set up for the exercise.



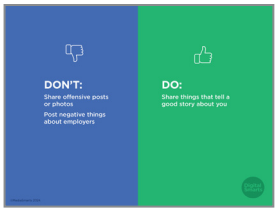
49. Everything we've talked about can help you manage your privacy online, but in the end you can't control it completely. No matter how carefully you use your privacy settings and how much you trust your friends, you have to assume there is always a chance that something you share online might be seen by the wrong people.

Before you post anything, ask yourself four questions: Is this how I want people to see me?

Could somebody use this to hurt me?

Would I be upset if they shared it with others?

What's the worst thing that could happen if I shared this?



50. These days, a lot of employers check social media when they're deciding whether or not to hire someone.

Don't post things that are offensive, racist or sexist. (That includes "liking" posts from friends with that kind of content.)

Don't post negative things about your current or past workplaces.

Do make sure to share things that you're proud of or that tell a good story about you. If you run a marathon or volunteer at the library, you can post about it.

Besides social networks, it can be useful to Google your name and see what comes up. You may want to add things like where you live or your workplace to the search to make it more specific.

51. Your friends are also trusting you to make good decisions about the things that they post. Before you share or like something that somebody else posted, ask these questions:

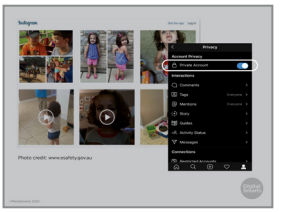
What might happen if what I'm sharing gets sent to people who weren't supposed to see it?

How will my friend feel if their families see it? Their neighbours? Their friends, girlfriends, boyfriends, husbands, wives, or partners?

If you're not sure it's okay to share, ask!

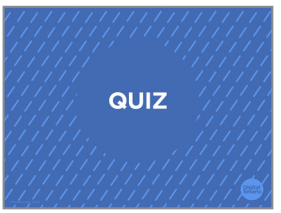
If there are other people in what your friend shared with you, think about this: How will they feel if I share this?

Is there anything they'd be worried about?



52. If you have kids or grandkids, think carefully about their privacy. Teach them good privacy habits by asking them if it's okay before you post anything about them and talk to them about who might see the photos and how long they could stay online.

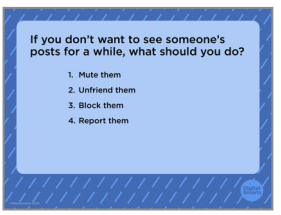
You should also make sure you limit access to these photos by using privacy settings, which we've spoken about during this workshop, so only family and close friends can see them.



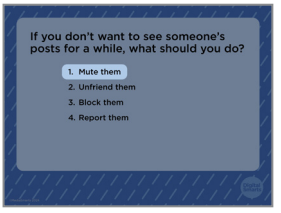
53. We'll do a quick quiz now to review what we've learned in the last section.

54. What does it mean when we say a social network is "open"? Does it mean that anyone can join? That it's free to join? That anyone can see what you post unless you block them? Or that there's no way to control your privacy on them?

55. We say a social network is "open" if the *default* is that anyone can see what you post online, unless you block them. As you've seen, though, there *are* ways to control your privacy on them.



56. If you don't want to see someone's posts for a while, what should you do? Mute them, unfriend them, block them or report them?



57. If you just don't want to see someone's posts for a while, the best option is to mute them. They won't be notified and when you're ready to see their content again, all you have to do is unmute them. You can still manually go look at their content. even if they're muted.

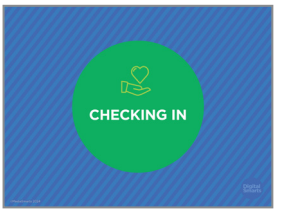
58. What's the best way to manage who can see what you post on a social network?

Using the privacy settings? Reading the privacy policy? Setting your account to Private? Or using a fake name when you sign up?

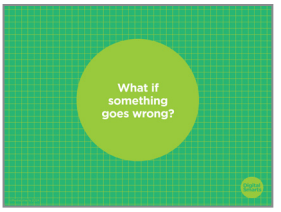
59. Managing who can see what you post is exactly what privacy settings are for.

60. When you're using those social networks, what is the fewest number of people you can share a post with? Your friends, some of your friends, just one friend or just you?

61. On most social networks, you can limit the audience of your posts to just you. Most of the time you'll want to share with more people than that, but sharing something that only you can see can sometimes be a good way of giving yourself time to think twice about who you really want to be able to see it.



62. Before we go on, let's pause for a moment to see if anybody wants to take a break or needs any support.



63. One of the most common reasons that people sometimes don't want to use the internet is because they're worried that something will go wrong.

The good news is that most of the time, it's easy to fix your mistakes.

64. If something private gets out of your control, there are a few different ways to fix it.

Your first step is usually to ask anyone who's shared it to take it down from their accounts. This works more often than not!

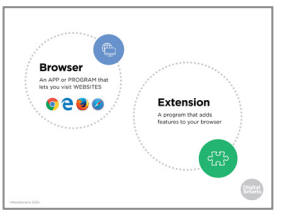
If that doesn't work, or you don't feel you can do it safely, you can report it to the place where it was posted (like Facebook or Instagram). Social networks won't often take down photos just because they're embarrassing, but if something is being used to harass you they might.

Sharing "intimate images" of someone – which means pictures where you're fully or partially naked – without their consent is against the law in Canada, no matter how old the person in the picture is, and a judge has the power to have it taken down.

You can also turn to the law if something being shared about you is defamatory, which means that it is not true, has been shared in a public place, and will hurt your reputation. Look for a free or subsidized legal clinic in your city for advice.

If you prefer, you can reach out to an anti-violence worker or your support networks to seek guidance on the options and resources available to you.

Finally, if the thing that went wrong is your fault, do whatever you can to fix it. No matter how mad someone is, an apology and a sincere effort to try to fix things will usually help.



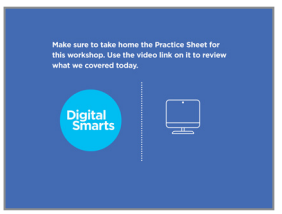
65. Before we finish, let's review some of the new terms we've learned in this session.

A browser is the app or program that lets your device visit web pages. Examples of browsers include Chrome, Firefox and Safari.

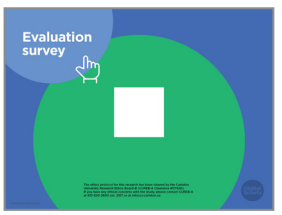
An extension is a little program that you add on to your browser that lets it do extra things.

66. We're almost done this workshop, so let's stop for a second to see if anybody has any questions about what we've covered so far.

If you'd rather not ask your question now, I will be here for a little bit after the workshop, so feel free to come ask me.



67. Make sure to take home the Practice Sheet for this workshop. Use the video link on it to review what we covered today.



68. Before we debrief, we ask that you please take five minutes to complete this program evaluation survey. This survey is similar to the one at the beginning of the workshop; it will help the team at MediaSmarts better understand if the workshop is doing a good job of supporting survivors' digital knowledge, skills and confidence, and inform future program updates. Your answers are completely anonymous. This survey is meant to evaluate the program, not you, the participants. There are no right or wrong answers; it is okay if you don't have the skills being asked about in the survey.

As before, your participation is completely voluntary. If you're interested in taking the survey, all you need to do is scan the QR code with your phone's camera, or type in the link on your browser to access it. We'll pause here again until everyone is finished, please take your time.

69. You are also invited to participate in an online interview discussion to provide further feedback on the workshops you are attending as part of this program. Interviews will take about 60 minutes. Interview participants will receive a $50 electronic gift card to PC/Shoppers as a thank you for their time. The MediaSmarts' team who developed this workshop will use these interviews to guide program updates and to assess the value and impact of this workshop.

If you'd like to participate, you can take a picture of this slide and use the link to register. You can also scan the QR code instead, it will open the registration page. You don't have to sign up now; you can save a photo of the slide or the registration link and decide to participate later.

70. We have come to the end of the workshop. We would like to check in with you before you leave:

Are there any immediate needs or concerns coming out of the workshop that we can help you with? If we cannot help, we will point you to some available resources that may be able to help.

Do you have any other questions coming out of the workshop? If we have the answer, we will give it to you. If not, we will point you to some available resources that might help or we will connect you with someone who might know.

Finally, let's end with a question: what is one skill you have learnt in this workshop that you think will be useful in your own life?