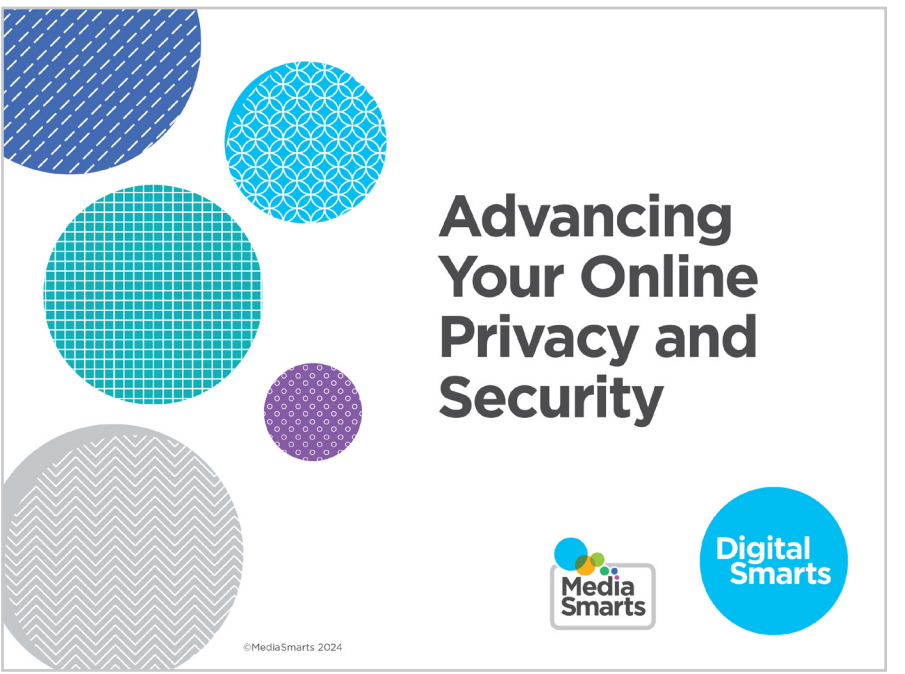
Workshop Script



Financial contribution from

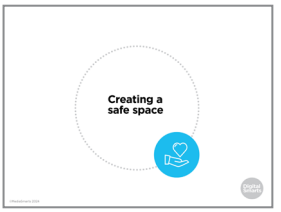
Public Health Agency of Canada
Agence de la santé publique du Canada

1. Welcome to our session on advancing your knowledge of online privacy and security. This workshop is designed to teach advanced skills in managing your privacy and protecting your devices.

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

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.

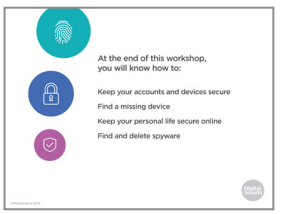


3. This workshop touches on some topics that may be upsetting, so before we get started, let's talk about how we can create a safe space here.

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.

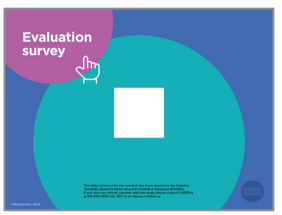


4. The focus of this workshop is on advanced skills to manage your online privacy and security. First, we will do a brief survey to help us understand what you know and what you do not know about advanced online privacy and security. Then we will cover the following topics and engage in some exercises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

Keep your accounts and devices secure; Find a device like a phone that's missing; keep your personal life secure online; and Find and delete "spyware" on your phone.

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 advancing 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.

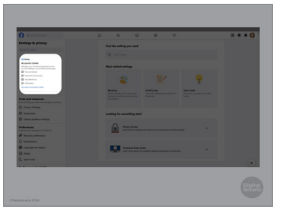
Your participation is completely voluntary. If you're interested in taking the survey, all you need to do is scan the QR code with your phone's camera, or type in the link on your browser to access it. We will pause until everyone who is interested has completed the survey; please take your time.

6. First, we're going to discuss how to keep your accounts and devices secure. You may have discussed some skills related to this topic in another workshop but we will review them again here.

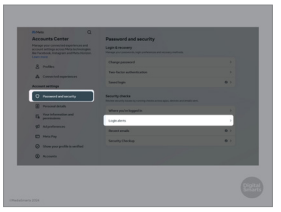
7. One tool you can use to keep your accounts secure is *two-factor* authentication. You may have already practiced this skill in another workshop but we are going to review it again here.

As well as entering your password, if you have two-factor authentication turned on you'll also get a text sent to your phone with a one-time code. You need to enter the code as well as your password to log in.

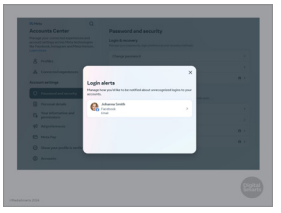
This means that somebody who gets your password can't get at your accounts. The drawback is that you can get locked out of your accounts if you lose your phone, and it may not be as useful if your phone is your main way of getting online.



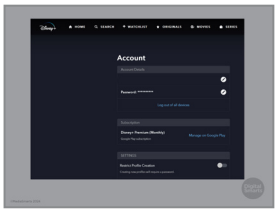
8. You can also set some social networks to let you know if a new device logs in to the account. In Facebook, go to Settings & Privacy and click on Accounts Center in the left-hand bar.



9. Then click on "Get alerts about unrecognized logins." That will let you know if anybody logs in to your account from a new device.

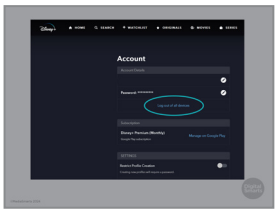


10. If you get that alert and it wasn't you that logged in, change your password right away.

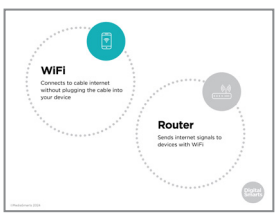


11. Most online services, like social networks and streaming services, also let you *log out* of every device you're logged in on.

If you have trouble finding this option, do a search for 'Sign out of all computers' and the network you want to log out of. For example, 'Sign out of all computers WhatsApp.'"



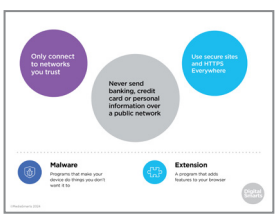
12. It's not a bad idea to do this now and then, just in case you've forgotten somewhere you're logged in.



13. A lot of us use public WiFi in places like libraries or coffee shops. It's usually safe to do most things on public WiFi, but it's important to know that public WiFi is less secure than your home network because you share it with many other people.

Networks that don't make you enter a password are especially risky because anyone can connect to them. That means that people with the right programs can see what you're sending to the router, including your login and password and other sensitive data like your credit card information.

A WiFi network is more secure if you have to enter a password to connect to it, but you're still sharing it with anyone else who might be connected. That means anyone else who is also connected that that network can potentially access anything you might be sharing in that network.

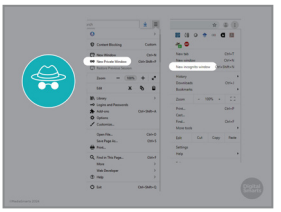


14. There are three things you can do to make using public WiFi safer.

First, make sure that you're using a network you trust. You can give your network any name you want, so people sometimes set up fake ones called things like "Public Library" or "Starbucks Wifi" to spy on people or install malware on their computers. Double-check to make sure you're connecting to the right network.

Second, never do anything requiring financial or personal information, like online shopping or checking your bank account, on public networks. Even on a secure network there's a chance that somebody might be able to see what you're sending.

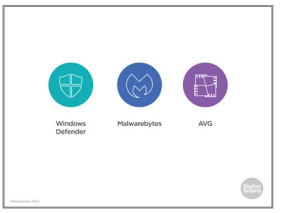
Finally, stick to secure sites as much as possible. Those are the ones with a padlock in the address bar and a web address that starts with https, instead of just http. If you're using an iPhone or iPad, you can turn on "Automatic HTTPS Upgrade" by going to the Advanced settings in Safari. Keep in mind, though, that having an https address doesn't mean the site itself is trustworthy – just that nobody else can see what you send them.



15. If you have to send important information on a public computer, try to use one that is connected with a network cable, like a desktop computer, instead of one that uses Wi-Fi. Make sure to do it in Incognito or Private Browsing mode so that the computer doesn't remember anything you typed or what websites you visited.

On most browsers, you open this mode by clicking a button on the top right and then choosing "New private window" or "New incognito window."

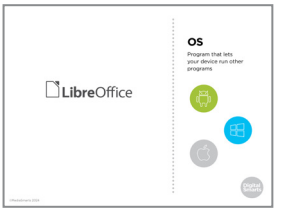
16. Just like you shouldn't connect to networks you don't know are trustworthy, never use a USB stick or memory card unless you bought it yourself or you know you can trust the person who gave it to you. These can easily spread malware from one computer to another. Sometimes people even leave infected memory sticks where people can find them to spread malware.



17. You should also make sure that you have anti-malware software running.

Windows machines come with a free, built-in program called Windows Defender. Make sure that it's turned on and that no other anti-malware programs are running – if you have more than one they can get in each other's way.

For Macs and mobile devices, install a reliable tool like Malwarebytes or AVG. These are free, but will try to get you to pay more to get extra services. Don't worry – the free version is probably all you need.

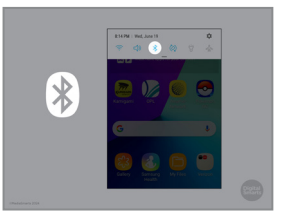


18. The companies that make programs frequently find and fix security problems in them. That's why it's important to set them to update automatically. That's especially true of browsers – since that's how you send most personal information – and operating systems such as Windows or iOS.

That also means that it's risky to use pirated versions of Operating Systems like Windows or programs like Microsoft Office, because you won't get these updates.

If you need to use programs like Word or Excel but can't afford them, use a free and legal alternative like Libre Office. This doesn't look exactly like Microsoft Office but it can read and save files in the same formats. That means you can read a Word file in Libre Office and save your files in a format that someone else can read with Word.

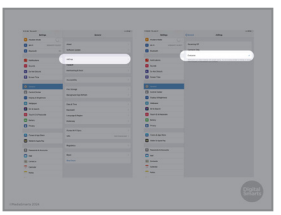
19. A lot of websites give you the option to log in with your Facebook or Google account instead of creating a new account to use them. This seems fast and convenient, but it also lets the website see everything that's in your account – your friends, what posts you've liked, and so on.



20. Finally, there are a few features on your devices that you should turn off when you're not using them.

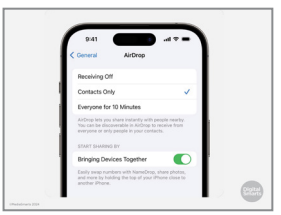
Bluetooth lets different devices connect wirelessly. It's useful for connecting to things like speakers or earphones, but it's also possible for other people to connect to your devices if it's turned on.

Some devices let you turn Bluetooth on and off just by tapping the Bluetooth icon. On others you need to go to Settings and turn it on or off there.

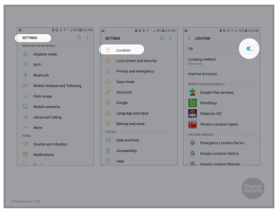


21. Apple devices also have a feature called AirDrop that lets people share files between devices. People can use this to put unwanted photos or other things on your device if you have it turned on.

To stop this from happening, go to Settings, then General, and then tap on Airdrop.

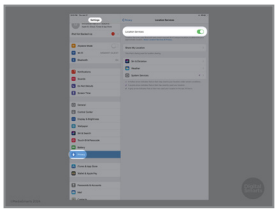


22. Then you'll see what the current setting is. If you want to control who can AirDrop things onto your device, set it to either Contacts Only – so only people you've pre-approved can do it – or just to Receiving Off. You can also set it to receive from anyone for 10 minutes, after which it will switch to Contacts Only.

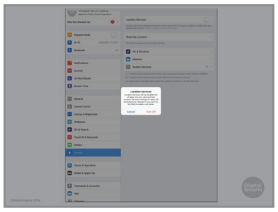


23. GPS is another feature you should turn off when you're not using it. It can be useful when you need to know where you are, but it can also send that information to websites you visit or apps that you're using.

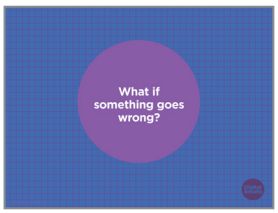
To do this on Android devices, go to Settings, scroll down to Location and tap it, and then switch the toggle to Off.



24. To turn off location on an iPhone or iPad, go to Settings and then tap Privacy.



25. Tap the Location Services slider and then Turn Off.



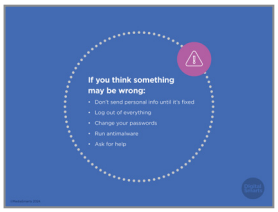
26. No matter how careful we are to secure our accounts and devices, there's always the chance that something can go wrong.

The good news is that most of the time, it's possible to fix things.

27. Here are a few signs that you might have a problem with your device or your accounts:

- If people get messages that you didn't send;
- If you frequently don't get messages that other people say they sent to you;
- If you can't log in to one or more of your accounts;
- Or if your device is unusually slow.

As well, if you get a notice about a login or a password change request that you don't remember it probably means somebody has tried to get at your accounts.



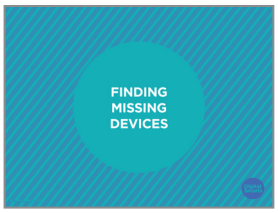
28. If you think that somebody might have accessed your device or one of your accounts – or might have tried to – this is what you should do:

First, don't send anything personal or sensitive until the problem has been fixed. Next, make sure all of your accounts are logged out on every device that you use.

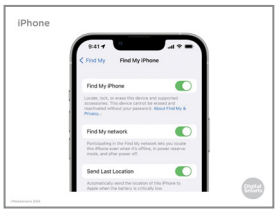
Change all of your passwords. Remember to make your email password totally separate from all your other ones.

Finally, run your antimalware software.

If you've been locked out of your device or any of your accounts, you may be able to get help from the company. So long as you can show that you are who you say you are, they should be able to put you back in control.

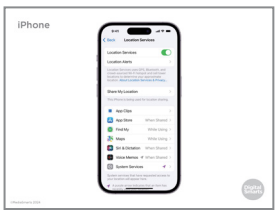


29. There are also ways to find your devices if they're lost or stolen.



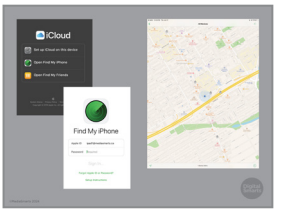
30. On an iPhone, go to Settings, then your device's name, and Find My. Sign in with your Apple ID or, if you don't know yours, tap "Don't have an Apple ID or forgot it?" and then follow the instructions.

"Find my iPhone" or "iPad" will let you see where a device is when it's turned on. "Find My network" lets you see it even when it's turned off.

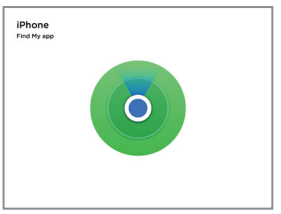


31. Next, go to Settings, then Privacy & Security, and then Location services, and make sure you've given the app Find My access to your location.

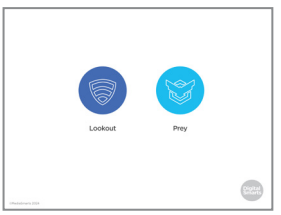
Keep in mind that this might allow other people who know your Apple ID and password to know your device's location! You'll need to decide whether knowing where your *device* is worries you more than somebody else knowing where *you* are.



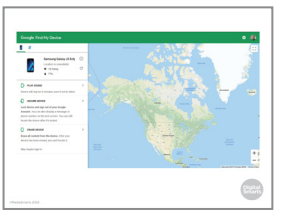
32. If the “Find My” settings have been enabled on your device before you lose it, it is possible to locate it. To find ~~it~~ your device, open iCloud.com on any browser, click on Find My iPhone and enter your Apple ID and password. You’ll then see a map with your device’s location on it.



33. If you have another iPhone or iPad, you can also use the Find My app – the icon looks like this – to do the same thing.



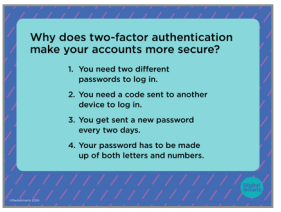
34. You can also set up apps on your device like Lookout and Prey that let you track, lock and wipe your devices if they’re lost. Like a lot of apps, the basic versions are free but some features cost extra.



35. Unfortunately, you can only find Android devices if you have GPS turned on. You’ll have to decide whether it’s more important for your privacy to keep your location hidden or to be able to find your phone.

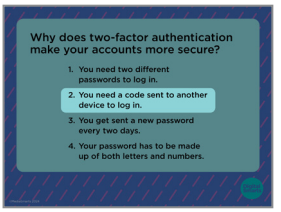
If GPS is turned on and Find My Device is turned on in Settings, you can find it by going to Android.com/find and signing into your Google account. As well as showing you where it is on the map you can lock the device or erase it from there.

36. Let’s do a quick quiz to check that you understood everything we just talked about.



37. Why does two-factor authentication make your accounts more secure?

Because you need two different passwords to log in? Because you need a code sent to another device to log in? Because you get sent a new password every two days? Or because your password has to be made up of both letters and numbers?

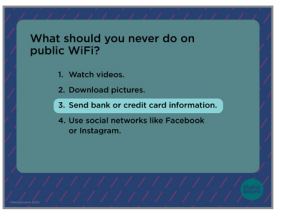


38. Right! With two-factor authentication, a code is sent to another device each time anyone enters your password. Nobody can get at the account without that code.

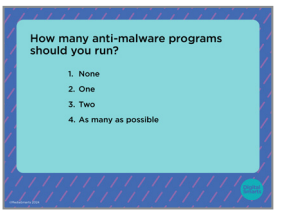
It is a good idea for your password to be a mix of letters, numbers and other characters – but you don't need to change passwords every two days.

39. What should you never do on public WiFi?

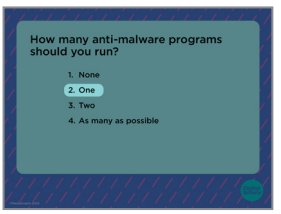
Watch videos? Download pictures? Send bank or credit card information? Or use social networks?



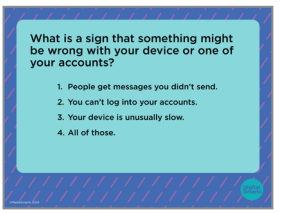
40. Right! It's usually safe to do most things on public WiFi, but don't send bank or credit account information. That means no online shopping, too!



41. How many anti-malware programs should you run? None; one; two, to be on the safe side; or as many as possible?

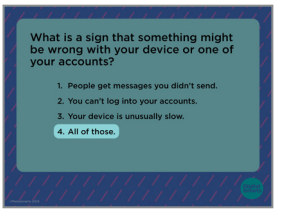


42. You do need an antimalware program, but it's best to just run one. More than one can actually get in each other's way.



43. Finally, what is a sign that something might be wrong with your device or one of your accounts?

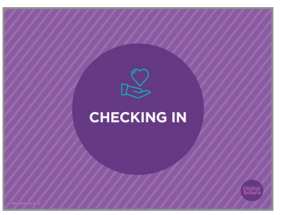
That people get messages you didn't send? That you can't log into your accounts? That your device is unusually slow? Or all of those?



44. Right! Those are all signs that you have a problem with your account or device and need to get help.

45. Try doing one of the things we've talked about in the last few minutes:

- setting up two-factor authentication;
- setting one of your social networks to let you know if somebody else tries to log in;
- turning off Bluetooth, GPS or AirDrop;
- Or finding your device remotely.



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

47. Of course, privacy and security aren't just about devices and accounts. A lot of our personal lives are online these days, and it's important to keep those secure as well.

48. Now let's talk about tips for protecting your information when online dating. It's never too early in a relationship to start thinking about safety.

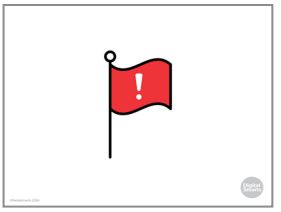
If you're using an online dating app, use a free webmail service like Gmail or Outlook to make a new email address, and use that to register the app. You can also make a disposable email address at Sharklasers.com or Protonmail.com. Both of those are good options for keeping your email address private when dating online. Keeping it separate from your main email address can help you keep things private.

Next, take a look at the dating app's privacy policy and terms of service. You don't always have to read the whole thing, but you should see whether you can totally delete your photos and other things you've posted after you close your account.

Once you make a connection with someone, don't share personal info – especially things that could be used to find you in real life, like an address or phone number – until you're comfortable with sharing that information.

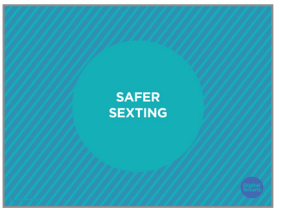
"Sweetheart" scams, where people ask you for money to help them leave their country or deal with other trouble, are common on dating sites. Never send money to anyone you've met on a dating site or app.

If you decide to meet someone you met on the app in person, have the first meeting in a public place and tell a friend or a family member that you're going. You can ask them to check in on you partway through, too, to give you an excuse to leave if things aren't going well.



49. It's also worth checking out what safety tools have been built into the dating site or app itself. How do you report something like harassment or being sent unwanted photos? How can you block someone if you need to?

It's important to trust your instincts when you're starting a relationship online. If someone is pressuring you or being aggressive about meeting in person, asking for photos, or getting angry if you don't respond to their messages, block them right away.



50. Sexting – sending naked or sexy photos of yourself to someone else – can be part of a healthy relationship but it can be risky as well.

51. Never send anyone a sext unless they've clearly told you they want to see it.

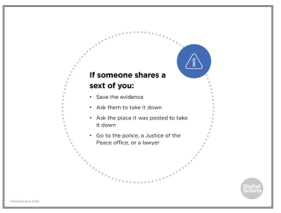
If you do send a sext, remember that there's no way to keep people from making copies of things online. Even if you use an app like Snapchat or Instagram reels that are no longer visible after a certain period of time.

Don't include your face, distinctive tattoos, or anything else that could be used to identify you.

If you get a sext that you didn't ask for, block the sender right away.

If you get a sext that you *did* ask for, don't share it or show it to anyone without the permission of the person in it.

And don't ever pressure someone to send you a sext if they don't want to.



52. If someone shared a sext of you without your permission, there are things you can do about it.

First, save the evidence. If it's been posted in a public space, get a screenshot. If you heard from someone that they saw it, get them on record.

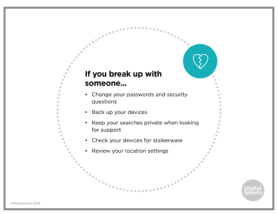
You can ask the person to stop sharing it or take it down. Even if they say no or don't answer, keep a record of the texts or emails so you can demonstrate that it was shared without your consent.

If it was shared somewhere like a social network or a website, email the site and ask them to take it down. Make sure to say that the photo violates the terms of service – nearly all sites have rules against posting sexts without the sender's permission. If you took the photo, you own the *copyright* to it, so you can ask to have it taken down on that basis as well.

In Canada, it's against the law to share "intimate images" of someone without their permission – no matter how old they are – and a judge can order the photos taken down and lay criminal charges against the person who shared them. You'll want to be prepared before you go to the police for this step: see the worksheet *Help! Someone Posted a Sext Without My Consent* or the YWCA guide on sexual image-based abuse for more tips.

If you want to have your image taken down but don't want to go through the police, you can go to the Justice of the Peace office at a courthouse or have a lawyer handle it for you.

Some cities have legal aid clinics that will help with cases like this for free or for a reduced fee.



53. Even if things are still friendly between you, it's always a good idea to change your passwords when you break up with someone. Even if you don't remember ever sharing any passwords with them, you should assume they know them.

Change the security questions you use when you forget your passwords, too: these are usually taken from things that a partner might have learned while you were dating – your first pet's name, for example – so play it safe and switch to something new.

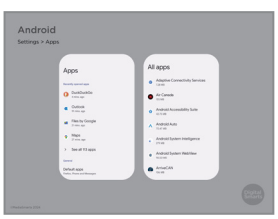
Another good precaution is to make backups of photos, files, and anything else that might be important to you, in case you may have to do a full reset of your devices later. You can back them up to a cloud service like Google Drive, to a USB drive, or both.

If you're looking for support in getting out of a relationship, use the things we've covered in this workshop (like using secure HTTPS sites) to keep your searches private.

Double-check to make sure your device doesn't have any "spyware" or "stalkerware," programs that tell someone else where you are or what you're doing.

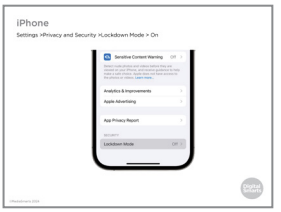
Now we'll take a look at how to do that.

54. On an iPhone, swipe left on the Home screen until you see the App Library. Tap the search box at the top of the screen, then scroll through the list of apps and remove anything you don't recognize.



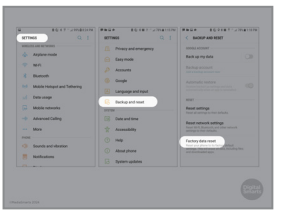
55. On an Android device, go to Settings > Apps > See all apps, or search for "Apps".

56. There are also apps you can use like Certo and Incognito that will scan your devices for spyware, but you should know that there is always a chance that spyware may still be on your phone.



57. If you have an iPhone you can also turn on Lockdown Mode, which protects you from most kinds of spyware. It also limits how much you can use apps like FaceTime and Safari.

To turn on Lockdown mode, go to Settings, then Privacy and Security, and then toggle Lockdown Mode to On.

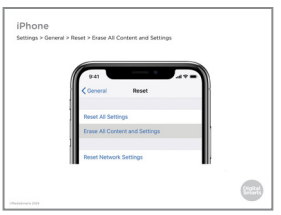


58. If you've done that and still think that your ex-partner may be tracking you, you may have to wipe your phone completely.

On an Android phone, go to Settings, then Backup and Reset, then Factory Data Reset. This will erase everything you've saved on the phone and every app that's been downloaded onto it.

Before you do that, write down all your important contacts – like phone numbers and email addresses of close friends or family members – and any other vital information on your phone onto a piece of paper, and keep that in a secure place.

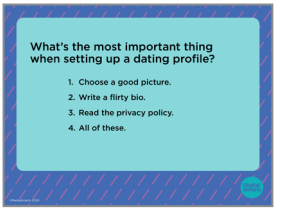
If you use your email address for two-factor authentication, you will need to reinstall your email app and log in again.



59. On an iPhone or iPad, tap settings, then General, then Reset. Then tap Erase All Content and Settings and enter your passcode or Apple ID.

Whatever kind of device you use, remember not to restore from a saved backup or cloud service after you reset it. That could re-install whatever spyware might have been on there.

60. Let's do another quick quiz to catch up.



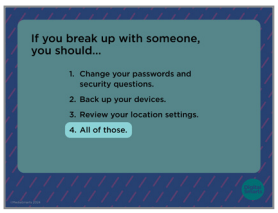
61. What's the most important thing when setting up a dating profile?

Choose a good picture? Write a flirty bio? Read the privacy policy? Or all of those?

62. Right! A picture and bio are important, but you need to check out what will happen to anything you upload if you decide to delete them.

63. If you break up with someone, is it important to..

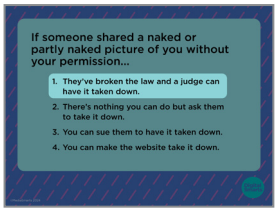
Change your passwords and security questions? Back up your devices? Review your location settings? Or all of those?



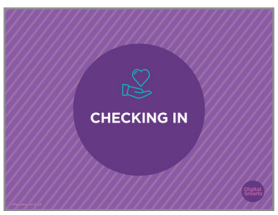
64. We share a lot of things with our partners, like our passwords and devices. When a relationship ends, make sure you're not sharing those any more.

65. If someone shared a naked or partly naked picture of you without your permission, which of these is true?

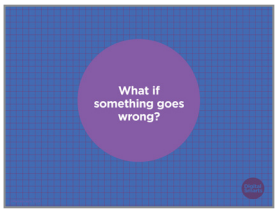
They've broken the law and a judge can order it taken down? There's nothing you can do but ask them to take it down? You can sue them to have it taken down? Or you can make the website take it down?



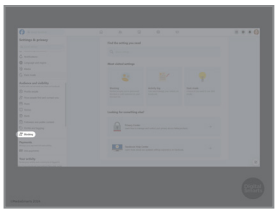
66. In Canada, it's a crime to share "intimate images" without the permission of the people in them, and a judge can order a website to take them down.



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



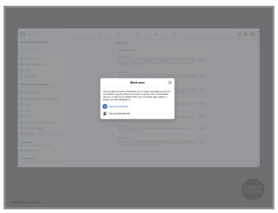
68. Despite all our best efforts, sometimes our private lives can go wrong online too. Here are some things you can do to help get things under control.



69. One of the first steps to deal with harassment is to block the sender.

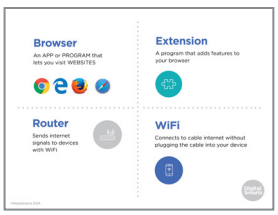
On Facebook, if you Block someone they can't send you a new Friend request, can't see anything on your profile, can't tag you and can't send you messages on that network.

To block someone, go to Settings and then pick Blocking on the left menu.



70. Then type the name of the person you want to block into "Block Users". Once you've chosen the right person click on Block.

Most other social networks and messaging apps have some form of blocking as well.

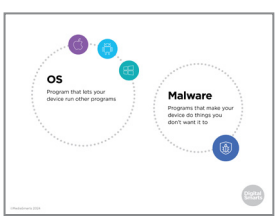


71. Before we finish, let's review some of the new terms we've learned in this session.

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.

WiFi sends internet signals to your computer without any kind of wires or cables by using a wireless *router* that's connected to cable internet.

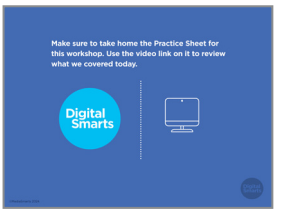


72. A device's OS, or Operating System, is what allows it to run other programs. The main types of OS for computers are Windows, Chrome, and Mac. The main types for mobile devices are Android and iOS (for iPads and iPhones).

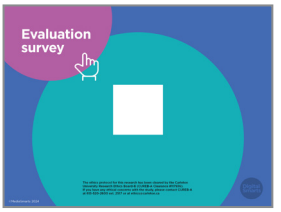
Malware means programs like viruses that do something to your computer that you don't want.

73. 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.



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



75. 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.

76. 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.

77. 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?