Workshop Script

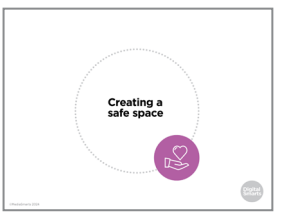
Financial contribution from

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

1. Welcome to our session on online relationship safety. This workshop is designed to help people who have experienced violence feel safer and more confident in managing their relationships and personal information 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 *[remote delivery: put your question into the chat]* any time you have a question along the way.

2. This workshop has 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

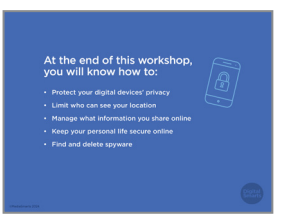


3. This workshop touches on some topics that may be upsetting, so before we get started, let's talk about how we can create a safe space here.

   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 how to safely navigate your relationships and personal information online. First, we will do a brief survey to help us understand what you know and do not know about protecting your privacy and managing online relationships. Then we will cover the following topics and engage in some exercises to practice these skills:

Protect your privacy and digital devices;

Limit who can see your location;

Manage what information you share online;

Keep your personal life secure online;

Find and delete “spyware” on your phone.

As we go through these topics, we will have four 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 knowledge and skills in protecting your online privacy and managing online relationships, 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.

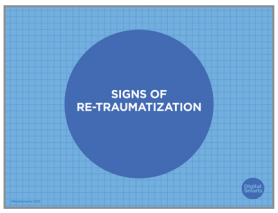
Your participation is completely voluntary. If you’re interested in taking the survey, all you need to do is scan the QR code with your phone’s camera, or type in the link on your browser to access it. We will pause until everyone who is interested has completed the survey; please take your time.

6. There are many types of abuse, which makes it difficult to have one blanket definition of abuse. In the context of relationships, abuse is a pattern of behaviours used to gain or maintain power and control over a partner — physical abuse (physical violence or threats of it) is just one example of such behaviour.

Other examples include emotional and verbal abuse (non-physical behaviours meant to control, isolate, and frighten), financial abuse (an abusive partner extending power and control into your financial situation), sexual abuse (forcing, pressuring, or coercing someone to do something sexually that they do not want to do), or technology-facilitated violence and abuse (TFVA). TFVA may be defined generally as a form of abuse or controlling behaviour involving the use of technology to coerce, stalk, surveil or harass another person.

(Individual) trauma is an event or circumstance resulting in physical harm, emotional harm, and/or life-threatening harm. Trauma has lasting adverse effects on an individual's physical, mental, emotional, social and spiritual health and well-being.

Re-traumatization is the reactivation of trauma symptoms via thoughts, memories, or feelings related to the past trauma experience. This may happen when, because of a triggering event, circumstances remind you of earlier trauma, or it may happen when you are speaking about a trauma.

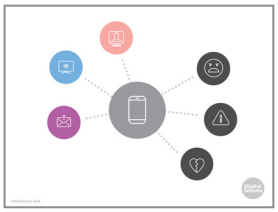


7. Some possible signs of re-traumatization are:

Negative thoughts that are associated with fear or other emotions experienced during the trauma; flashbacks; dissociation; trouble concentrating; feeling "on edge," very anxious, tense, or easily startled; fatigue; experiencing distress or strong physical reactions e.g. fast breathing and heartbeat or sweating; feeling withdrawn, distant, and isolated; intense feelings of guilt, anger, fear, sadness, shame, or despair; feeling unable to control your emotions, such as not being able to calm yourself down, a decreased sense of security.

For in-person delivery: 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. Remember to give us a thumbs-up before you do so we know if you are OK or if you require assistance.

For remote delivery: We encourage you to turn off your microphone and camera if you feel distressed and need to take a moment to self-regulate. Please remember to use the thumbs-up emoji (found in the reactions tab) before you do, so we know if you are OK or if you require assistance.

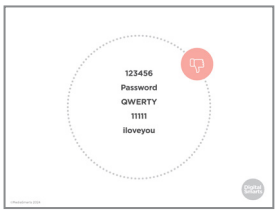


8. Today a lot of our lives—including our relationships—happens online. There are a lot of good things about being online: it can help us stay connected with distant friends and family and help us meet new people who share our interests.

But there are risks too. Technology can be used to abuse, to harass and to spy on us, so we need to be aware of how to keep ourselves and our devices safe.

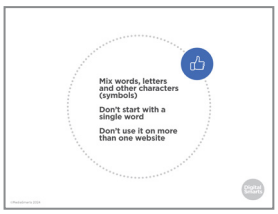
9. Let's talk about some of the important steps you can take to secure your devices.

One of the most important steps for staying safe in relationships online is something that we all should be doing anyway—keeping our accounts and devices secure.



10. The best way to keep your accounts and devices secure is to use a good password.

Don't use any of the common passwords shown on this slide. Ways of unlocking a device like your fingerprint or facial recognition aren't secure either, except in combination with a password, because someone who has access to your phone could point it at your face or touch your fingertip to it.



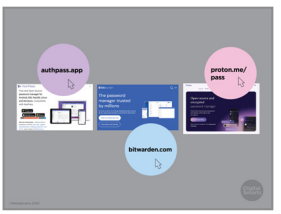
11. But even if you're not using one of the most common passwords, and your password isn't something that people could easily guess, there is a difference between weak and strong passwords.

What makes a password strong comes down to three things.

First, it isn't made up of just one thing – a strong password combines words, letters, and symbols.

Second, it isn't based on a single word.

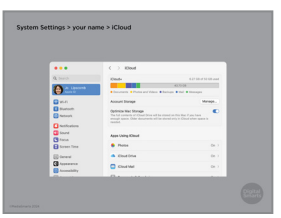
Third, you don't use it on more than one site.



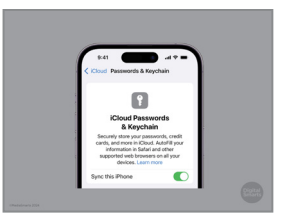
12. Another option is to use a *password manager*. This is a program that you use to handle your passwords for different accounts. It creates a different, almost unbreakable password for each account and then handles logging in to them for you.

Password managers can be useful, but they only solve the problem of having different passwords for different accounts. You still need to make sure you have a strong password for the password manager, because anyone who can log into the password manager can log into all your accounts.

One popular password manager that has a free basic version is Bitwarden.



13. Apple devices like iPhones and Macs also have their own built-in password manager, which you can use if you have an iCloud account. To use it, first go to System Settings, then click on your name and then iCloud. (On older devices you may have to click Apple ID and then iCloud.)

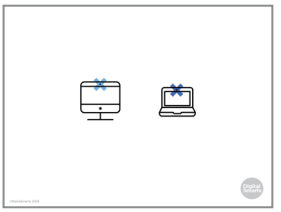


14. Then turn on Passwords & Keychain.

15. Another tool you can use to keep your accounts even more secure is *two-factor* authentication.

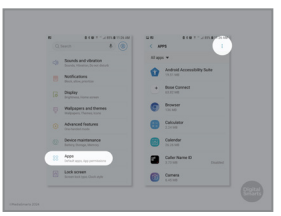
As well as entering your password, if you have two-factor authentication turned on you'll also get a text sent to your phone with a one-time code. You need to enter the code as well as your password to log in.

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 doesn't help much if your phone is your main way of getting online.

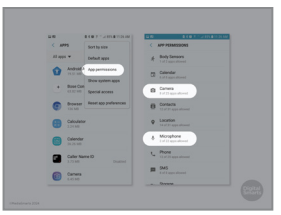


16. Another way to secure your device is to cover the cameras on laptops and other devices when you're not using them so that you can't be seen by them when you don't want to be. You can do this with a sticker or something similar that's easy to take off when you want to use the camera.

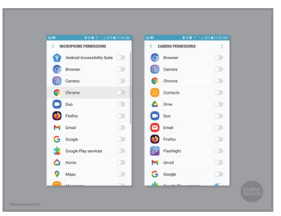
17. Turning off the microphone on your devices is a bit trickier, but it's a good habit too. We'll walk through how to do this on a mobile device.



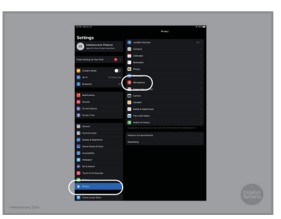
18. On Android devices, tap Settings (the gear icon) and then Apps. Tap the three dots at the top right of the screen.



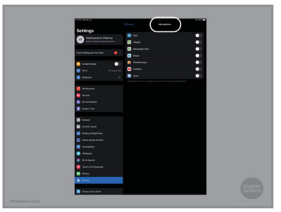
19. In the window that pops up, tap App Permissions. Now you can tap Microphone or Camera.



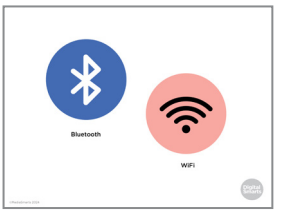
20. Now you can see any apps that have access to the microphone or the camera. Slide them to the left to turn them off – you can always turn them back on later.



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

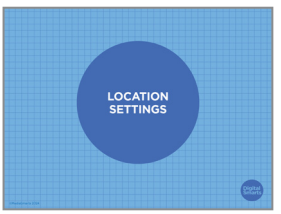


22. Next, tap Microphone and slide everything to the left. You can do the same with the camera.



23. Bluetooth and WiFi make your device visible to other devices. These are on by default, so when you're not using them, turn them off by going into Settings or tapping the Bluetooth and WiFi icons.

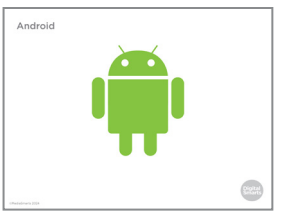
You can also go to your Bluetooth settings (Settings > Bluetooth) and look for any devices that are paired with your phone. If there are any you don't recognize, unpair them.



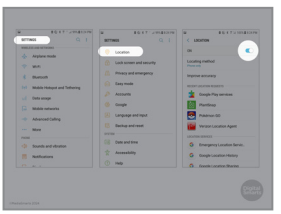
24. Phones are also set by default to share your *location* – where you are. The main way they do this is through the Global Positioning System, or GPS.

This can be a real privacy and security risk, so it's important to know how to turn your location settings off.

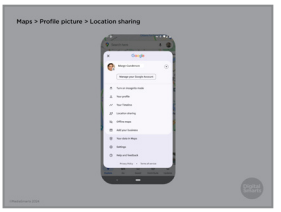
GPS sends a signal that shows where your device is. You should turn it off when you're not using it. It can be useful when you need to know where you are, but it can also send that information to websites you visit or apps that you're using.



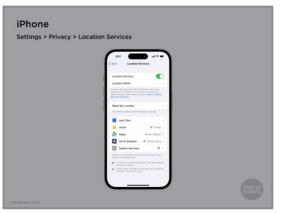
25. To turn off location tracking on Android devices, you need to turn off GPS like we saw how to do a few minutes ago with the microphone and camera settings.



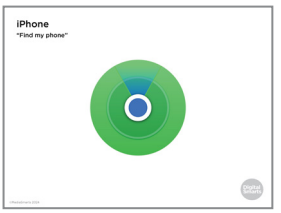
26. To do this, go to Settings, scroll down to Location and tap it, and then switch the toggle to Off.



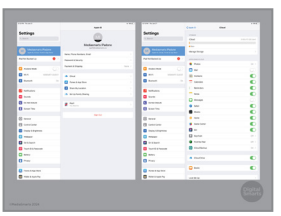
27. You can also keep specific people from seeing your location. To do that open Maps, tap your profile picture and then Location sharing. Tap the profile picture of anyone who shouldn't see your location, and then tap "Stop".



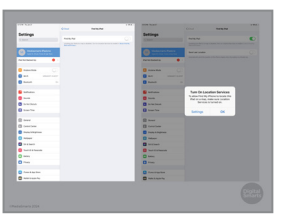
28. On an iPhone, open Settings > Privacy > Location Services or search for "Location Services" and turn off location sharing.



29. Location sharing and apps like "Find my Phone" still work if your phone is turned off, so you have to switch off these specific apps in the settings.

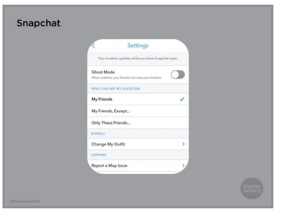


30. For iPhones or iPads you need to turn off "Find my iPhone" or "Find my iPad." To do that, click on Settings, then tap the name of the device at top left.

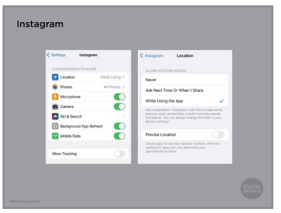


31. Next, tap the Find my iPad or Find my iPhone slider and tap OK in the box that pops up.

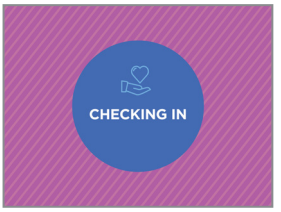
32. Some social media apps share your location, too. Let's look at how you can turn that off.



33. Snapchat shows where you are on a map. To turn that off, open Snapchat and tap your profile icon. Next tap the three vertical dots at the top right and scroll down to the "Who Can..." section. If you tap "See My Location" a pop-up will appear that says "Ghost Mode." Toggle that to "On".

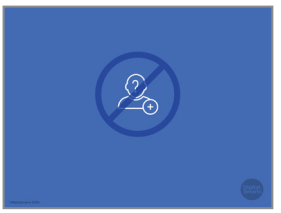


34. On Facebook or Instagram, you can turn location off by tapping Settings > Privacy > Location Services and then tapping the Toggle next to it. Most other social networks put location in similar places within settings like "Privacy" or "Safety".



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

36. Now let's look more broadly at how you can manage your privacy on social networks.



37. From a privacy perspective, there are two kinds of social networks: *closed* ones like Facebook, where two people have to mutually agree to be connected, and *open* ones like Twitter where you can follow someone without them necessarily following you back.

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.

38. 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 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.

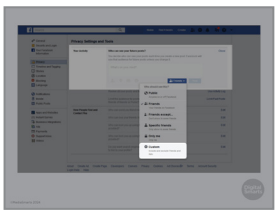
We will walk through how to adjust these settings on Facebook.

39. To change your settings on Facebook, click Settings and then click on Privacy on the left menu. Find "Who can see your future posts" and click "Edit."

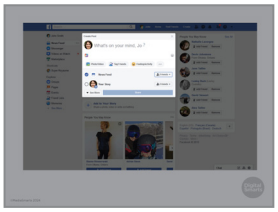
40. You can set it to public, which means that people who aren't your friends see your posts – not a good idea because this leaves you with the least amount of privacy.

You can also choose "friends except" to leave some friends out or set it to "specific friends" so that just some of your friends see your posts, or "only me" so that only you can see them.

"Only me" 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.



41. You can control who sees your content with each post, too, by choosing "custom" in the drop down menu.

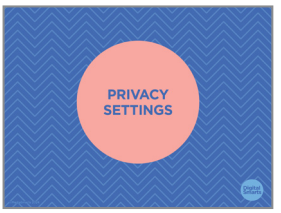


42. If you want, you can let all your friends see most of what you post but share some posts with just a few friends– or even just one person.

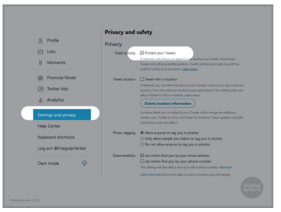
43. A lot of social networks let you "tag" a post or photo with someone's name. What that means is that anybody looking for you on that network will see anything posted with your name.

If you click Timeline and Tagging in the left menu, you can decide who can see posts tagged with your name. That means you can keep friends-of-friends from seeing them.

You should also set it to let you know anytime you're tagged in a post or photo. That way you can ask someone who posts a photo of you to take it down right away if you don't like it.

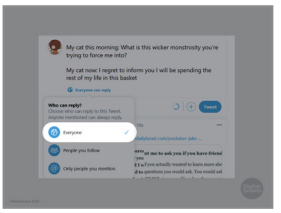


44. You can also set custom *privacy settings* on your social networks.



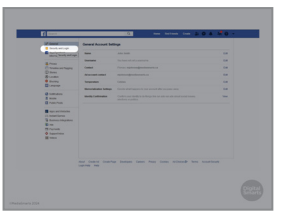
45. It's harder to control who sees what you post on an open network like X (formerly Twitter), where anyone can follow you, but most of them offer a tool like X's "Protect your Posts" which makes people get your permission to see your tweets.

To do that on X, click on Profile, then click Privacy and Safety and tick the box that says: "Protect your Posts."

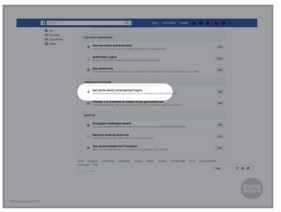


46. You can also control who is able to reply to your tweets. Before posting, click or tap on "Everyone can reply" and then choose who you want to reply.

47. You can also adjust the settings in some social networks to let you know if a new device logs in to your account.

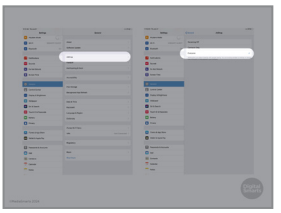


48. In Facebook, go to settings and click on Security and Login in the left-hand bar.



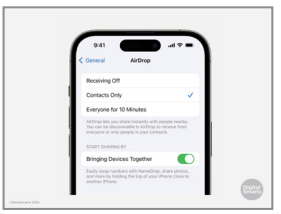
49. Then click on “Get alerts about unrecognized logins.” That will let you know if anybody logs in to your account from a new device by sending an email to the address you used when you signed up.

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



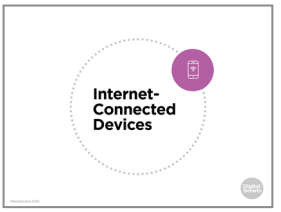
50. Apple devices also have a feature called AirDrop that lets people share files between devices. People can use this to put unwanted photos or other things on your device if you have it turned on.

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



51. 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. (Off is probably your best choice because it offers you the most privacy.)

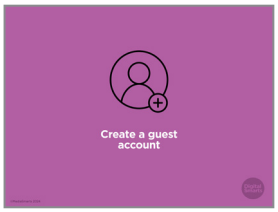
You can also set it to receive from anyone for 10 minutes, after which it will switch to Contacts Only.



52. Internet-connected devices, including smart speakers like Amazon Echo and Google Home, are another privacy risk. You can’t turn the microphone on these devices off because they have to listen for the command that will “wake” them, like “OK Google” or the device’s name “Alexa”.

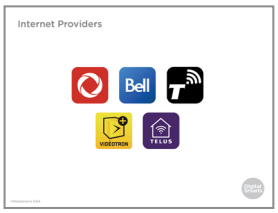
If you have connected devices like these, be aware that they can be used to spy on you. You can disconnect them from the WiFi or power them down if you need to have a conversation that won’t be overheard, or you can have the conversation outside of the home.

Wearable devices like smart watches or even GPS-enabled key chains can be a privacy risk too. Even pet locators can make it possible for people to find out where you are.

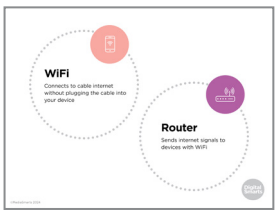


53. Here are some tips for managing your privacy when using "smart" devices:

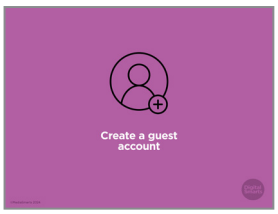
Create a guest account on your WiFi. Keeping the device off your main WiFi account limits what it can collect.



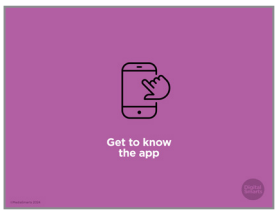
54. Your internet provider - for example Rogers, Bell, Telus, Videotron or TekSavvy - may have come with an app that lets you change your internet router settings.



55. Your *router* is what sends wireless WiFi signals to your devices. If you have home internet, the company you get it from probably rents you your router.



56. That app should have an option to create a guest network. If there isn't an app, contact your internet provider to ask for help.



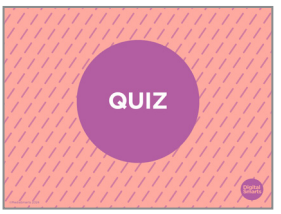
57. It's also useful to *get to know the app.* Because most smart devices don't have screens, they almost all have an app that you install on a phone or tablet. The app is how you change the different settings on the device. A lot of the privacy steps you can take involve changing the app settings, so it's a good idea to get familiar with the app and how you use it. Let's take a closer look at some of those settings now.

58. Change the wake word. Smart speakers also have a "wake word" that tells it to start listening to you, like "OK Google" or "Alexa." To make sure that it doesn't "wake up" by accident, change the wake word. (Not all smart speakers let you change the wake word. Some devices give you a limited range of wake word options, so pick the one that's the best fit.)

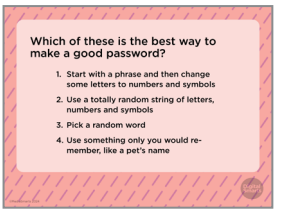
Turn off microphones and cameras when you don't need them. Many smart devices that have microphones or cameras have either physical switches or options in the app to turn them off.

Cover cameras when you're not using them too. Most smart devices that have cameras have a light that turns on when the camera is active, but to be on the safe side you should put a sticky note or something similar over any smart device whose camera doesn't need to be running all the time.

Finally, if you're considering getting something like a smart doorbell for security reasons, keep in mind that different devices collect more or less information than others. Look for one that only stores video locally (on a hard drive or memory card) instead of uploading it to the company.

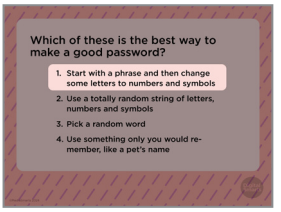


59. Let's do a quick quiz to check that you understood what we've covered.



60. Which of these is the best way to make a good password?

Start with a phrase and then change some letters to numbers and symbols? Use a totally random string of letters, numbers and symbols? Pick a totally random word? Or use something only you would remember, like a pet's name?



61. A random word is too easy to guess, and a totally random set of letters, numbers and symbols is too hard to remember. And anyone who knows you might know something like your pet's name.

Instead, start with a phrase – like "I like bananas" – and change some letters to numbers and symbols (like exclamation marks.)

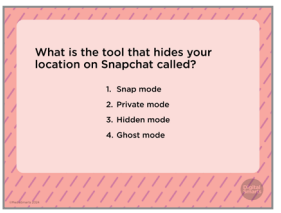
62. What are the benefits and risks of two-factor authentication? Is it more secure, but harder to use? It costs less than other methods but is less secure? Is it more secure, but you could get locked out? Or is it more secure, but you need a phone to use it?

63. It is more secure, but you could get locked out with two-factor authentication.

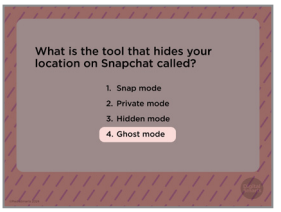
You don't need a phone for two-factor authentication, just another device that can access the internet. You can also get a device like a Yubikey that gives you physical two-factor authentication: plugging the device into your phone or computer, or tapping it, works the same as putting in a confirmation code.

Most two-factor authentication apps, like Google Authenticator or Microsoft Authenticator, are free. They can sometimes be a bit tricky to set up but are generally not that hard to use.

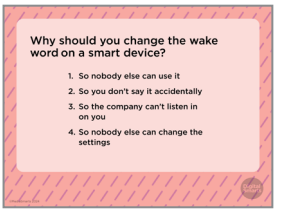
The bigger risk, though, is that if you lose access to the second factor – your phone, the app, or your Yubikey – you might get completely locked out. For instance, if you lose your phone you won't be able to get a code by text, and if you aren't able to access your email account you won't be able to get it by email.



64. What is the tool that hides your location on Snapchat called? Snap mode, Private mode, Hidden mode, or Ghost mode?



65. Ghost mode! If you have Snapchat on your phone, switch it to Ghost mode so people can't see where you are.



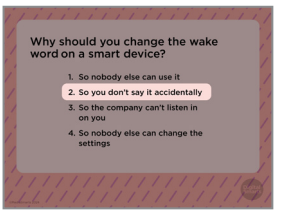
66. Why should you change the wake word on a smart device?

So nobody else can use it?

So you don't say it accidentally?

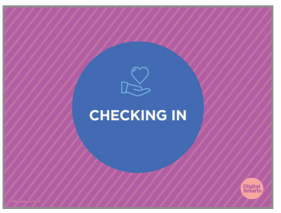
So the company can't listen in on you?

Or so nobody else can change the settings?



67. The main reason to change the wake word is so that you don't say it accidentally.

Unfortunately, changing the wake word doesn't keep the company from knowing what you say to your smart devices. It might keep other people from using it—until they hear you use the wake word.



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

69. Now let's talk about how you can keep your personal life secure.

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.

70. Let's start by talking about protecting your personal information. Some information should never be shared online. These are things that make it possible for someone to access your bank account or get a new credit card in your name.

You should never share:

- Your full name (including middle names)
- Your full date of birth (including the year)
- Your Social Insurance Number
- Your mother's maiden name (a lot of people use that as a security question)
- Your credit card information
- And your driver's licence or passport number

71. 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.

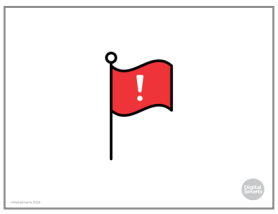
If you're using an online dating app, use a free webmail service like Gmail or Outlook to make a new email address, and use that to register. You can also make a disposable email address at Sharklasers.com or Protonmail.com. Both of those are good options for keeping your primary email address private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

Next, take a look at the 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.

72. "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.



73. It's also worth checking out what safety tools have been built into the dating site or app itself. For example: 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. We'll talk about how to do that a bit later in the workshop.

74. 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.

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

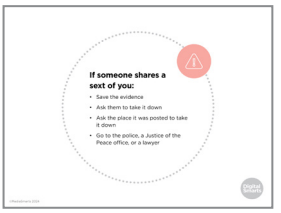
If you do send a sext, remember that there's no way to keep people from making copies of things online. Even if you use an app like Snapchat or Instagram reels that are no longer visible after a certain period of time, someone could take a screenshot of the content.

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.



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

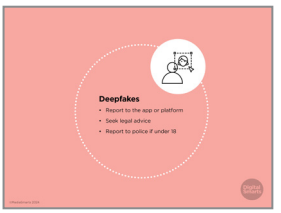
First, save the evidence. If it's been posted in a public space, get a screenshot. If you heard from someone that they saw it, get them on record.

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.

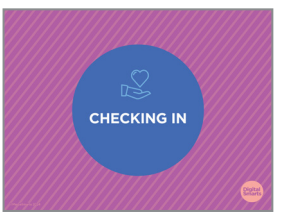
In Canada, it's against the law to share "intimate images" of someone without their permission – no matter how old they are – and a judge can order the photos taken down and lay criminal charges against the person who shared them. You'll want to be prepared before you go to the police for this step: 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.



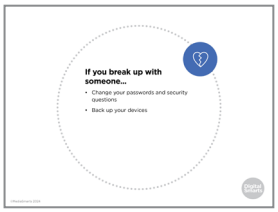
77. Another risk is deepfakes – photos or videos that show you doing something that you never did. Deepfakes that put women in pornographic scenes are becoming more common, and ordinary women and girls are often victims – not just celebrities.

Unfortunately, it's not yet clear whether the law against sharing non-consensual intimate images applies to deepfakes. If you are over 18 and you appear in a deepfake, your best response is to report it to the app or website where it was posted. (Most commercial pornography sites have policies against nonconsensual deepfakes.) If that doesn't work, you can look into taking action under civil law: consult a lawyer or legal aid clinic to see your options. (If you are under 18, the photo or video is still legally child pornography even if it is AI generated.)



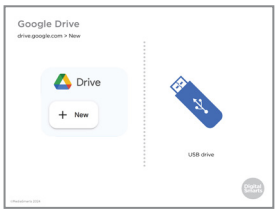
78. Before we go on, let's pause for a moment to see if anybody wants to take a break or needs any support.

79. Our online lives are a part of how relationships end, too.



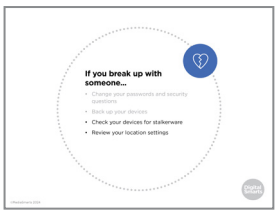
80. Even if things are still friendly between you, it's always a good idea to change your passwords when you break up with someone. Even if you don't remember ever sharing any passwords with them, you should assume they know them. Change the security questions you use when you forget your passwords,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



81. To upload files to a Google account, go to "Drive.google.com" and then select the "New" button at top left. You can upload individual files or a whole folder, so it will save you time if you put everything you want to upload into a single folder first.

A USB drive is a physical drive that you plug into your computer. It will appear as a folder that you can copy files into. Because it plugs into the computer's Universal Serial Bus (USB) port, you can't use a USB drive with most phones.



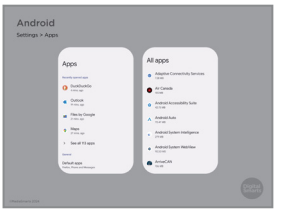
82. If things aren't that friendly and you're looking for support in getting out of a relationship, use the things we've covered in this workshop to keep your searches private. (There's more on that in the Explore Online Privacy workshop.)

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.

Some spyware has obvious names like "Mobile Tracker" or "Spy Tracker," but in general you should be cautious of any apps on your device that you don't recognize.

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

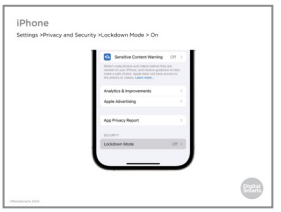
83. On an iPhone, swipe right on the Home screen until you see the App Library. Tap the search box at the top of the screen, then scroll through the list of apps and remove anything you don't recognize.



84. On an Android device, go to Settings > Apps > See all apps, or search for “Apps”.

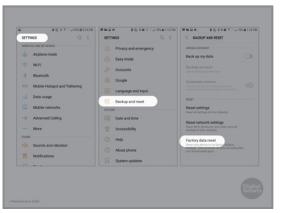
Use a search engine to look up the names of any apps you don’t recognize. If the search shows that it’s spyware – or doesn’t show that it’s a legitimate app – uninstall it.

85. There are also apps you can use like Certo and Incognito that will scan your devices for spyware.



86. 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.



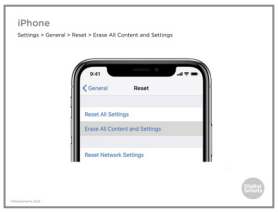
87. None of these methods are a hundred per cent effective, though.

If you’ve done that and still think that your ex-partner may be tracking you, the only absolutely sure way of getting rid of spyware is to do a “factory reset” and 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.

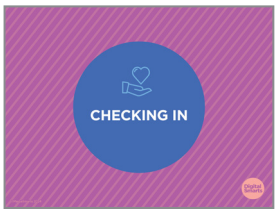
Before you do that, write down all your important contacts – like phone numbers and email addresses of close friends or family members – and any other vital information on your phone onto a piece of paper, and keep that in a secure place. That’s because a factor reset erases everything on your phone, including all of your apps and contacts.

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



88. 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 was on there.



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

90. Like everything else, relationship abuse has moved online as well.

Let's talk about what online relationship abuse is and how to recognize it.

91. One thing about online relationship abuse is that we may not always recognize that it *is* abuse. Some abusive behaviours are made to look romantic by media like movies or TV shows, and abusers also will often say they're doing these things out of love – or that you need to go along to show that you love and support *them*.

Here are some things that your partner should never do, or ask you to do:

- Make you share your password, or any other private information
- Share private photos or videos of you
- Pressure you to send photos or videos you don't want to, or to agree to sharing them with other people
- Expect you to always let them know where you are and what you're doing, or pressuring you to share your location
- Spy on you or stalking you online
- Make you unfriend people on social networks
- Spread rumours about you online

- Send messages that make you uncomfortable or scared
- Or threaten to do any of those things.

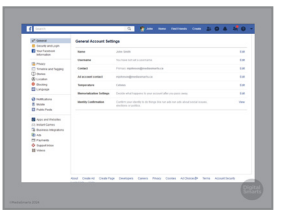
For more information, you can visit Tech Safety Canada's Technology and Safety Toolkit.

92. It's important to get evidence of online harassment in case you decide you want to seek legal help.

The most secure way of doing this is to get a screenshot. You can find out how to take screenshots on different devices and browsers at take-a-screenshot.org. If you think there's a chance that the device you're using might not be secure, transfer the screenshots to something like a USB drive or an external hard drive.

Whether you're dealing with harassment, spyware, deepfakes or your sexts being shared, it's important to keep a record of everything that's happened that you can give to the police or a lawyer if you decide to take legal action. You can use the *Evidence Chart* that comes with this workshop to do that.

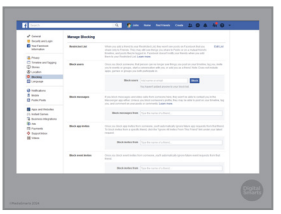
If doing this is too upsetting or distressing, ask someone you trust to help you do it.



93. You don't have to keep dealing with online harassment, though. Once you've saved evidence of what's happened so far you can block the sender. Blocking someone doesn't delete all of your old private messages.

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.



94. 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.

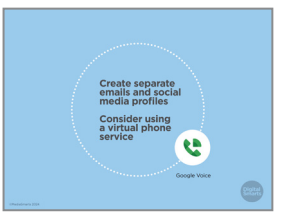
95. If you have left a relationship and need to hide yourself from your former partner, there are steps you can take to stop them from finding you online. You probably won't have to do this forever, but it can be an important temporary step to keep you safe.

Even on open networks like X (formerly Twitter), there are ways of locking them to private. Review your friend or follower lists to make sure you know and trust everyone on them.

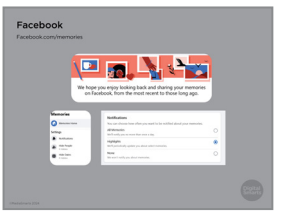
You can also create new accounts to use until you feel safe. If you do, use a new name that nobody would guess was you and use a generic profile picture like a sunset. Give a different city as your location in your profile.

Don't post about work, school, family or anything that would make you easier to find, and don't tag your posts or photos with your location. (Turning off GPS on your device is a good way to automatically keep them from being tagged with your location, but it's also important to check both before and after every post to make sure your location wasn't added.)

If you want to post about a place you went or an event you attended, wait to do it until afterwards, when you're no longer there.



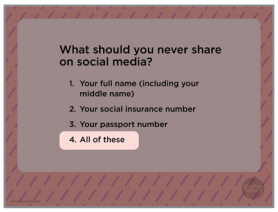
96. If you don't want to completely cut off contact with your ex-partner – for instance if you have shared custody of children, if you are still working out how to divide assets, or if you want to be aware of their mood and mental state – consider creating separate email or social network accounts just to stay in touch with them. You can use Google Voice or a similar virtual phone service for voice calls.



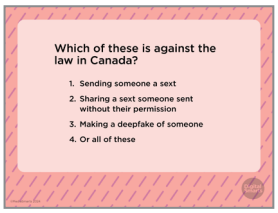
97. After you leave an abusive relationship, you may also want to change your social network settings to avoid seeing "memories," or old posts that might be distressing. On Facebook, for instance, you can go to Facebook.com/memories to change your notification settings or hide particular people or dates.

98. Let's do a quick quiz to check that you understood what we just covered.

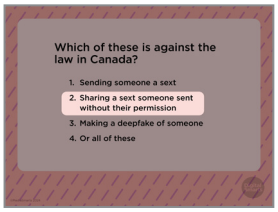
99. What should you never share on social media?
Your full name, including your middle name?
Your social insurance number?
Your passport number?
Or all of these?



100. That's right – sharing any of those things online can give people access to your accounts or let them pretend to be you.



101. Which of these is against the law in Canada?
Sending someone a sext?
Sharing a sext someone sent without their permission?
Making a deepfake of someone?
Or all of these?



102. Sharing a sext – what the law calls an "intimate image" – that someone sent without their permission is illegal in Canada, no matter what age the person in the sext is.

Besides criminal penalties, a judge can also order that the sext be taken down anywhere on the internet.

It's not a crime to send someone a sext, so long as they wanted to see it. (If they don't, that could be harassment.) Even senders who are under 18 are very unlikely to be charged just for sending a sext .

At the moment, it's not clear yet whether the law against sharing intimate images applies to deepfakes.

103. What does it mean to set your social media account to private?
That nobody can see what you post?
That only your closest friends can see what you post?
That only people you approve can see what you post?
Or that your posts disappear after 24 hours?

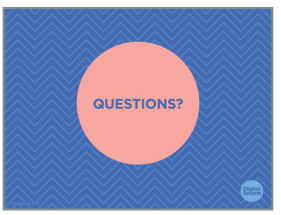
104. Right, only people you approve can see what you post. Even if you use a public-by- default social network like TikTok, you can control who follows you and sees your content by setting your account to private.

105. What is spyware?
Is it computer viruses that can infect your device?
Apps that let someone else see what's happening on your device?
Smart speakers that listen when they're turned off?
Or devices that let people see and hear what's happening in your home?

106. Spyware is apps on your device that let someone else spy on you. Remember, if you don't recognize an app, uninstall it.

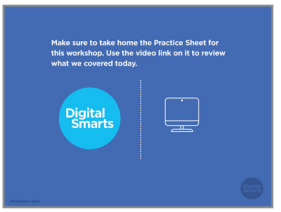
107. Windows computers come with a free, built-in program called Windows Defender. Make sure that it's turned on and that no other anti-malware programs are running – if you have more than one, they can get in each other's way.

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.



108. 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.

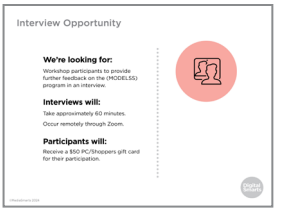
If you'd rather not ask your question now, I will be here for a little bit after the workshop, so feel free to come ask me.



109. Make sure to take home the Practice Sheet for this workshop. You can use the video link on it to review what we covered today.

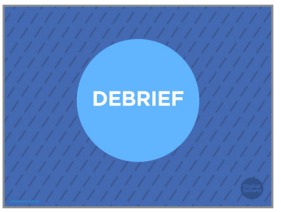
110. Before we debrief, we ask that you please take five minutes to complete this program evaluation survey. This survey is similar to the one at the beginning of the workshop; it will help the team at MediaSmarts better understand if the workshop is doing a good job of supporting survivors' digital 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.



111. 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.



112. 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?