Digital Smarts

Workshop Script

With funding from
Canada

Media Smarts

YWCA CANADA
A TURNING POINT FOR WOMEN
UN POINT TOURNANT POUR LES FEMMES

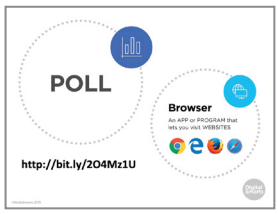
1. Welcome to our session on navigating online privacy.

We're going to have some time for questions at the end, but I'd also like to invite you to just raise your hand any time you have a question along the way.

2. Before we get started, I'd like you to think for a minute about what you're hoping to learn in this workshop.

You don't have to answer out loud. Just think about – What are some things you like to share on the internet? What are some things that you'd like to keep private?

What are some things you'd like more control of?



3. Before we get started, let's do a quick poll to find out how much you already know.

You can answer the first question by raising your hand -- how many people here are using devices, such as phones or computers, that you brought with you?

How many people are using devices that you haven't used before?

If you've got a device you already know how to use, start it up and use your browser to go to the website on the screen. Once you're there you can do the poll. It should only take a few minutes.

If you haven't used your device before, look for one of the browser logos you see on the screen. Then you can put in the web address to go to the poll.

I'll come around and help make sure everyone is able to get to the poll. If you finish ahead of other people, you can help one of your neighbours.

4. We covered a lot of the basics in the *Explore Online Privacy* workshop, so now we're going to dig a little deeper into how to keep your accounts and devices secure.

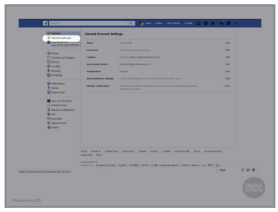
If you haven't attended that workshop, don't worry! I'll help you catch up on anything you missed that you don't already know.

5. We talked about making a good password in the *Explore Online Safety* workshop.

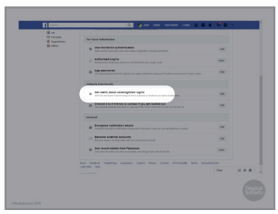
Another tool you can use to keep your accounts even more secure is *two-factor* authentication.

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.

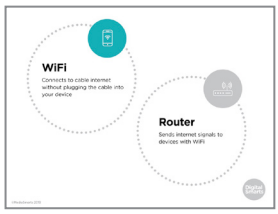
This means that somebody who gets your password can't get at your accounts. The drawback is that you can get locked out of your accounts if you lose your phone, and it doesn't help much if your phone is your main way of getting online.



6. 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 and click on Security and Login in the left-hand bar.



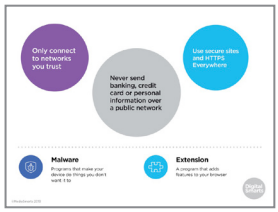
7. Then click on "Get alerts about unrecognized logins."



8. A lot of us use public WiFi in places like libraries or coffee shops. It's important to know that public WiFi is less secure than your home network.

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 things like your credit card information.

It's more secure if you have to enter a password to connect to the network, but you're still sharing it with anyone else who might be connected.

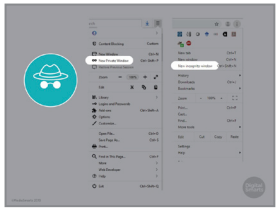


9. There are three things you can do to make using public WiFi safer.

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 with the right network.

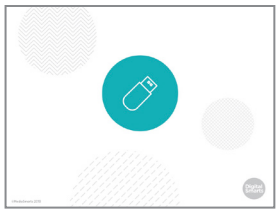
Second, never do anything like online shopping or checking your bank account on public networks. Even on a secure network there's a chance that somebody might be able to see what you're sending.

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. You also should install the HTTPS Everywhere extension, which tells websites to only connect you with the secure version of the site. If you're using an iPhone or iPad, you can turn on "Automatic HTTPS Upgrade" by going to the Advanced settings in Safari.



10. 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."



11. 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 on purpose.

12. 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.

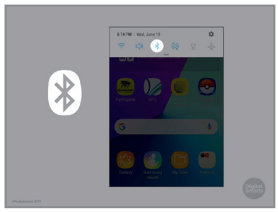
For Macs and mobile devices, install a reliable tool like Malwarebyte or AVG. These are free, but will try to get you to pay more to get extra services.

13. 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 OSes 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.

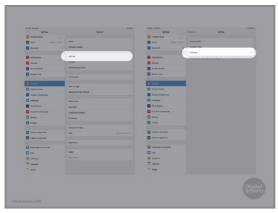
14. A lot of websites give you the option to log in with your Facebook or Google account instead of creating a new account to use them. This seems fast and convenient, but it also lets the website see everything that's in your account – your friends, what posts you've liked, and so on. Is it really worth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



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

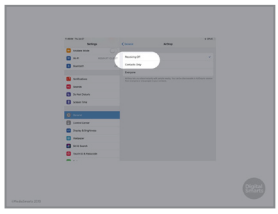
Bluetooth lets different devices connect wirelessly. It's useful for connecting to things like speakers or earphones, but it's also possible for other people to connect to your devices if it's turned on.

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.

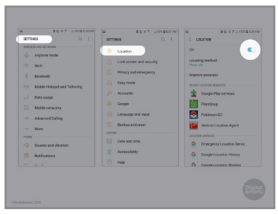


16. Apple devices also have a feature called AirDrop that lets people share files between devices. People can use this to put unwanted photos or other things on your device if you have it turned on.

To stop this from happening, go to Settings and then tap on Airdrop. Then you'll see what the current setting is.

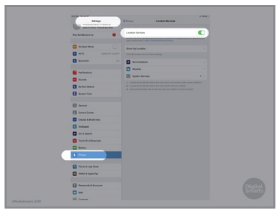


17. If you want to control who can AirDrop things onto your device, set it to either Contacts Only – so only people you've pre-approved can do it – or just to Receiving Off.

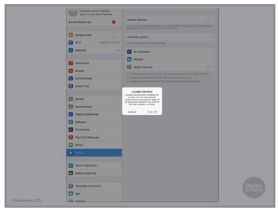


18. GPS is another feature you should turn off when you're not using it. It can be useful when you need to know where you are, but it can also send that information to websites you visit or apps that you're using.

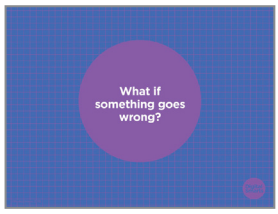
To do this on Android devices, go to Settings, scroll down to Location and tap it, and then switch the toggle to Off.



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



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



21. 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.

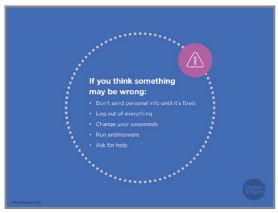
22. Here are a few signs that you might have a problem with your device or your accounts:

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.



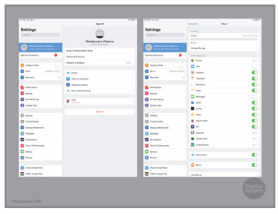
23. If you think that somebody might have accessed your device or one of your accounts – or might have tried to – this is what you should do:

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.

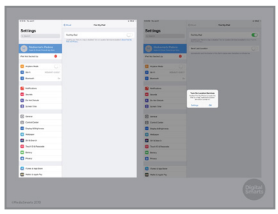
Finally, run your antimalware software.

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.

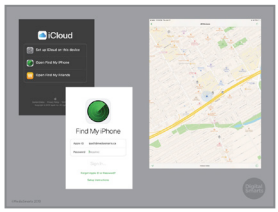


24. There are also ways to find your devices if they're lost or stolen.

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

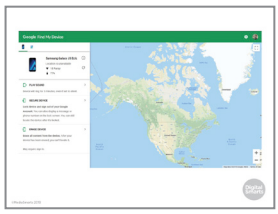


25. Next, tap the Find my iPad or Find my iPhone slider and tap OK in the box that pops up.



26. To find it, 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.

27. You can also set up apps 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.



28. Unfortunately you can only find Android devices if you have GPS turned on. You'll have to decide whether it's more important to keep your privacy or to be able to find your phone.

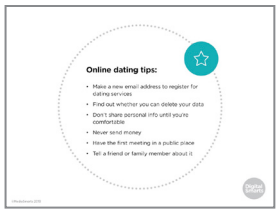
If GPS is turned on and Find My Device is turned on in Settings, you can find it by going to Android.com/find and signing into your Google account. As well as showing you where it is on the map you can lock the device or erase it from there.

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

30. 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.

31. 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.



32. A lot of people use apps to meet people they're interested in dating. Here are a few tips for doing that safely.

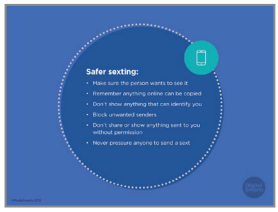
First, use a free webmail service like Gmail or Outlook to make a new email address, and use that to register. Keeping it separate from your main email address can help you keep things private.

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.

"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.



33. Sexting—sending naked or sexy photos of yourself to someone else—can be part of a healthy relationship, but can be risky as well.

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

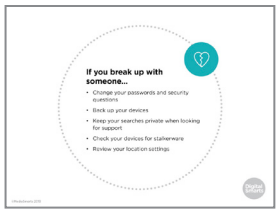
If you do send a sext, remember that there's no way to keep people from making copies of things online. Even if you use an app like Snapchat.

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 (we look at how to do this in the *Explore Online Privacy* workshop). If you have an Apple device, turn off AirDrop.

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.



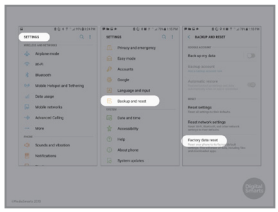
34. Our online lives are a part of how relationships end, too.

Even if things are still cool 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. You can back them up to a cloud service like Google Drive, to a USB drive, or both.

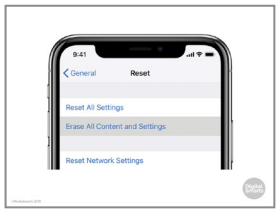
If things aren't that cool and you're looking for support in getting out of a relationship, use the things we've covered in this workshop (like using secure HTTPS sites) to keep your searches private. (There's more on that in the Explore Online Privacy workshop.)

Double-check to make sure your device doesn't have any "stalkerware," programs that tell someone else where you are or what you're doing. Uninstall any apps you don't recognize and go into App Permissions in the Settings menu to find out which apps can see your location. Review your location settings - so your location can't be tracked.



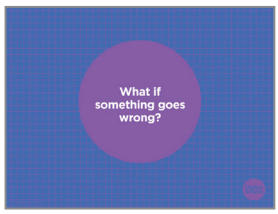
35. If you've done that and still think that your ex-partner may be tracking you, you may have to wipe your phone completely.

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.



36. 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.

37. Let's do another quick quiz to make sure you understood all that.



38. 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.

39. 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 show later that it was shared without your consent.

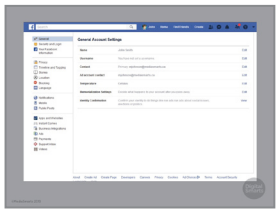
If it was shared somewhere like a social network or a website, email the site and ask them to take it down. Make sure to say that the photo violates the terms of service – nearly all sites have rules against posting sexts without the sender's permission. If you took the photo, you own the *copyright*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

40. If someone is stalking or harassing you online, the law can help you there too.

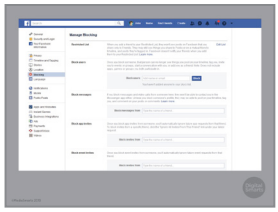
Harassment is contacting someone in a way that makes them feel physically or psychologically unsafe, or makes them worry that someone they know might be unsafe.



41. 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.



42. 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.

43. Before you block someone, though, make sure to save the evidence of what they're doing.

If you don't want to see the messages or texts in your inbox, make a special folder for them.

As well as keeping copies if you can, you should also get screenshots of anything a harasser sends you. The website take-a-screenshot.org gives detailed instructions on how to take screenshots on any device and OS.

Beyond blocking someone, you can also report what they're doing to the app or website where it's happening. You can also report it to your internet or phone provider, which can block their number or Internet Protocol address from contacting you.

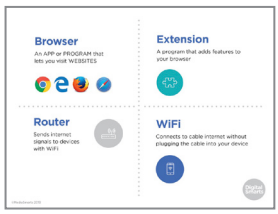
If you've blocked someone who's harassing you, be careful about accepting new friend requests. It's easy for people to set up new accounts.

Just like sexts, you can report harassment to the place where it's happening and also to the police or a Justice of the Peace.

A lawyer can also help you get a peace bond that will keep the person from contacting you in any way. Peace bonds work a bit

differently in different provinces, so you will want to get some kind of legal advice.

Your local women's shelter is a good source of information on how to deal with harassment.

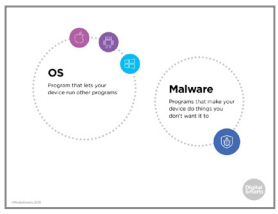


44. Before we finish, let's review some of the new terms we've learned in this session.

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.

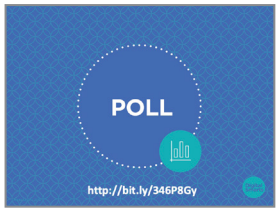


45. A device's OS, or Operating System, is what allows it to run other programs. The main types of OS for computers are Windows, Chrome, and Mac. The main types for mobile devices are Android and iOS (for iPads and iPhones).

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

46. 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.



47. We've covered a lot in this workshop. Now we'd like to hear from you about what you learned, what you still questions about, and your suggestions for how to make the workshop better.