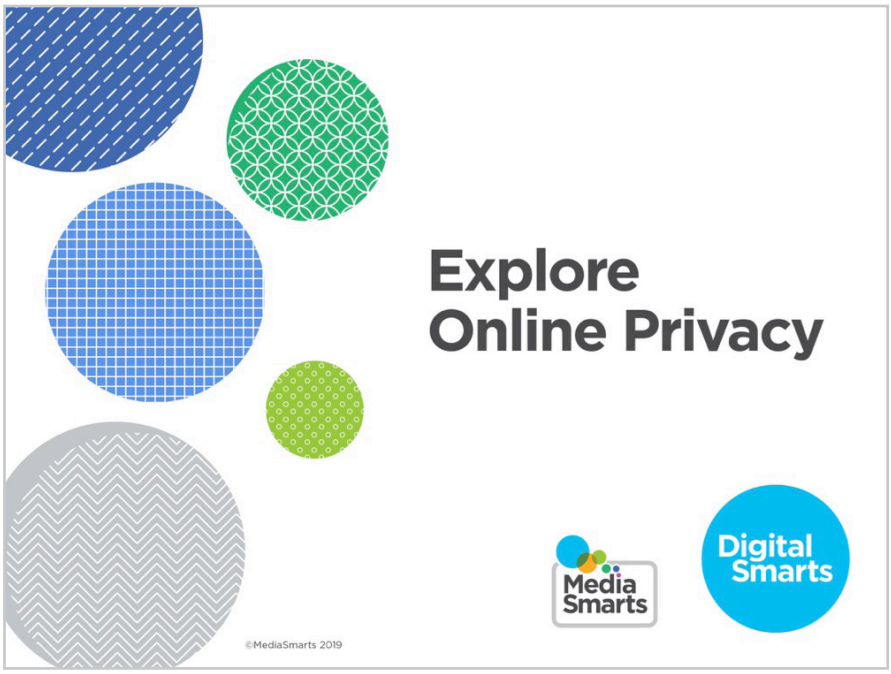
Digital Smarts

Workshop Script



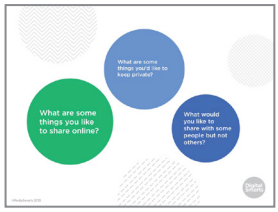
With funding from
Canada

Media Smarts

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

1. Welcome to our session on exploring online privacy.

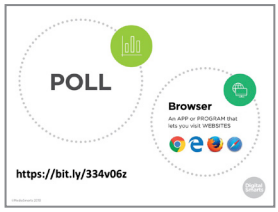
We're going to have some time for questions at the end, but I'd also like to invite you to just raise your hand any time you have a question along the way.



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?

How do you think the internet could help you do those things?



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.

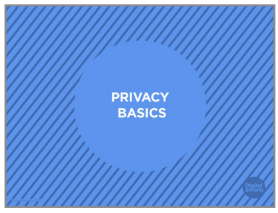
4. At the end of this workshop, you will know how to...

Protect your privacy online;

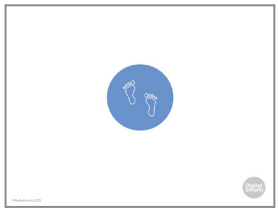
Use privacy settings on social networks;

Make good decisions about sharing things online; and Fix common things that can go wrong online.

© MediaSmarts 2019



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



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

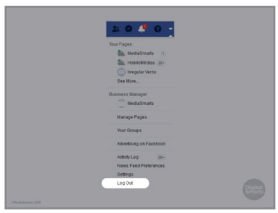
Sometimes we know when we leave these footprints, like when you share a photo. Sometimes you may not know what a website or app knows about you after you use it.

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

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

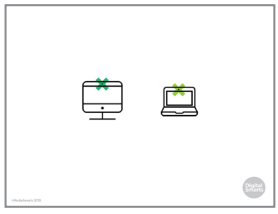
For example, you should never post things like credit card numbers, bank information, or passwords anywhere online except when your bank's website or a shopping site you trust and that you know is secure.

8. You'll know a site is secure because the web address ends in https (not just http) and there's a picture of a padlock in the address bar.



9. It's also important to make sure that you log out of online accounts when you're done with them, especially on shared devices.

Just closing the tab or window isn't enough: if someone using the same device goes to that page and you haven't logged out, they'll be able to use your account.



10. You can also 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 sticky note or something similar that's easy to take off when you want to use the camera.

© MediaSmarts 2019

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

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

Just remember that it doesn't usually stop the websites from recording what you do there.

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

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

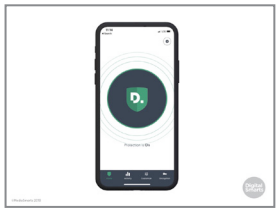
The best ways to do this are to use a browser that's designed to give you more privacy, like Firefox or Brave, and to use extensions that protect your privacy.

Extensions are little programs that work with your browser.

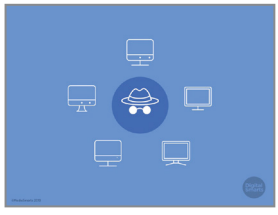
To find extensions on Firefox, click on Add-Ons and then search for the extension you want.

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

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



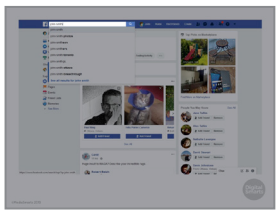
14. There's also a Disconnect app you can get for iOS or Android devices.



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

© MediaSmarts 2019

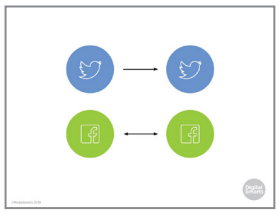
16. Now that we've covered the basics, let's talk about keeping yourself private when you're using social networks.



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

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

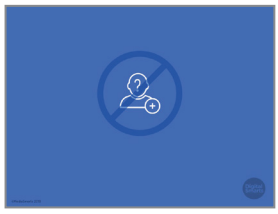
Once you've started to make connections, a lot of social networks also suggest people they think you might know or might want to connect with.



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

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

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



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

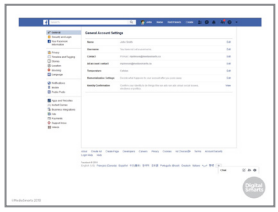
Don't accept friend requests from people you don't know or don't trust.

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

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

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

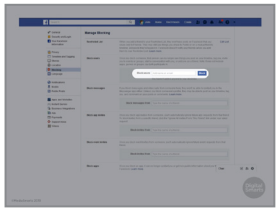
© MediaSmarts 2019



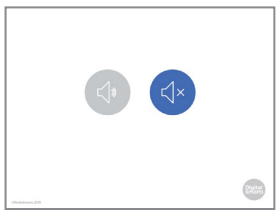
21. If you want to totally cut off contact from someone you can Block them.

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

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



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



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

People aren't told that you've muted them, so your friend who's posting pictures from her beach vacation won't be offended if you mute her until she gets back.

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

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

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

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

Is it open or closed?

Does it have a safety centre?

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

© MediaSmarts 2019

Are its terms of service readable? If not, is there a readable version of them somewhere online?

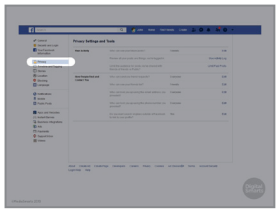
Now turn to the person next to you and compare notes. What answers did you get? How easy was it to find the information? What impression of the social network did you end up with?

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

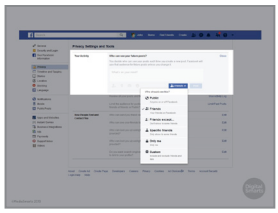
Almost all networks also have privacy settings that give you a bit more control over who sees what you post.

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

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



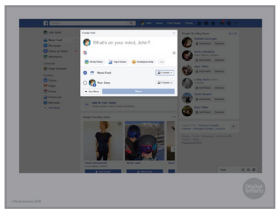
27. To change your settings on Facebook, click Settings and then click on Privacy on the left menu. Find "Who can see your future posts" and click "Edit."



28. Now you can set it so that people who aren't your friends see your posts – not a good idea.

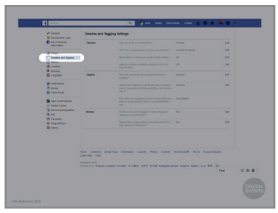
You can also leave some friends out, or set it so that just some of your friends see your posts, or so that only you can see them.

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



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

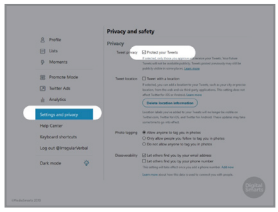
© MediaSmarts 2019



30. 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.



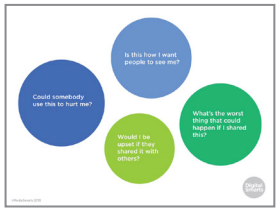
31. It's harder to control who sees what you post on an open network, but most of them offer a tool like Twitter's "Protect my Tweets" which makes people get your permission to see your tweets.

To do that on Twitter, click on your profile picture, pick Settings and Privacy, then click Privacy and Safety and tick the box that says "Protect your Tweets."

32. We'll do a quick quiz now to make sure you're caught up.

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

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



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

Before you post anything, ask yourself four questions:

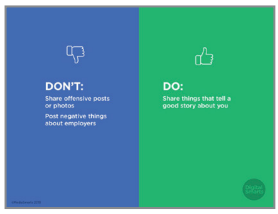
Is this how I want people to see me?

Could somebody use this to hurt me?

© MediaSmarts 2019

Would I be upset if they shared it with others?

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



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

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

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

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

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

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

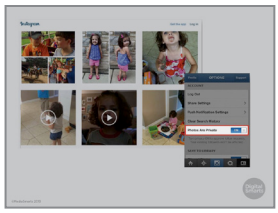
What might happen if what I'm sharing gets sent to people who weren't supposed to see it?

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

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

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

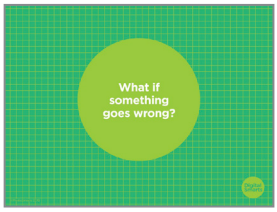
Is there anything they'd be worried about?



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

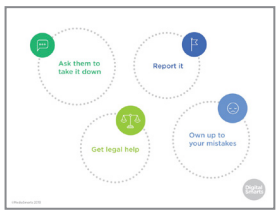
You should also make sure you limit access to these photos by using privacy settings so only family and close friends can see them.

© MediaSmarts 2019



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

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



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

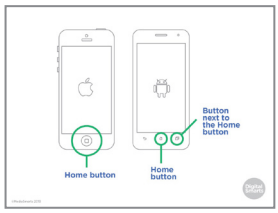
Your first step is usually to ask anyone who's shared it to take it down from their accounts. This works more often than not!

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

Sharing "intimate images" of someone – which means pictures where you're fully or partially naked – is against the law in Canada, no matter how old the person in the picture is, and a judge has the power to have it taken down. If that happens to you, report it to the police.

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

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



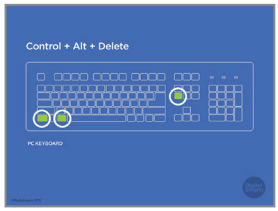
40. On phones and tablets you can usually exit an app without closing it by pressing the Home button.

If you want to close an app on the iPhone or iPad, push the Home button twice. Then use your finger to swipe the app you want to close off the screen.

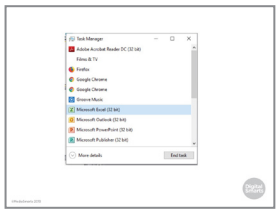
If you have a more recent iPhone or iPad with no home button, swipe young finger halfway up from the bottom of the screen and then lift your finger. This will open a new window where you can close apps.

On an Android device, tap the square next to the home button, then swipe the app off the screen. (Sometimes this is on the right, sometimes on the left.)

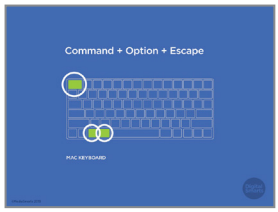
© MediaSmarts 2019



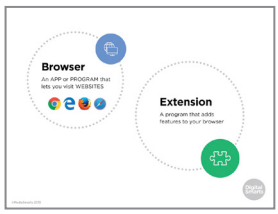
41. If you're using a PC, press Control, Alt and Delete.



42. That will bring up this Task Manager window. Click on the program that you want to close and press End task.



43. If you're using a Mac, press Command, Option and Escape instead.



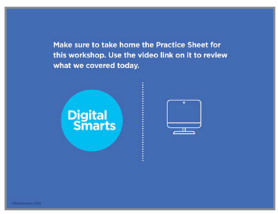
44. Before we finish, let's review some of the new terms we've learned in this session.

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

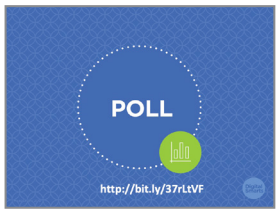
An extension is a little program that you add on to your browser that lets it do extra things.

45. 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.



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



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

© MediaSmarts 2019