Digital Smarts

# Workshop Script


*Financial contribution from*

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

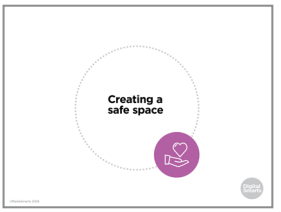
Media Smarts


**1.** Welcome to our session on discovering online safety. This workshop is designed to introduce some essential skills for keeping yourself safe 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 is accompanied by a number of support materials, including a practice sheet and video to help you remember the key content.

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




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

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

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

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


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

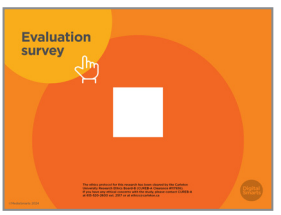
Make a strong password that you can remember.

Safely get new apps and programs for your devices.

And learn to recognize the most common ways that people try to cheat you on the internet.

As we go through these topics, we will have three scheduled breaks to allow us to pause and check in. We will end the workshop with another brief survey to help us understand whether this workshop improved your skills in managing your online safety, 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. It's not news that the internet can make it a lot easier to do things like watch TV and movies, keep in touch with friends and family, and find important information. More and more, you need to use the internet to access government services or apply for a job.

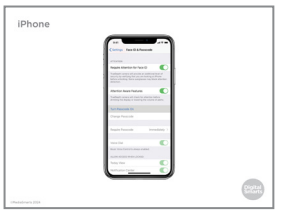
   But there are things to be careful about when using the internet: identity theft, computer viruses, and scams are some examples.

   The good news is that you can protect yourself from most of these risks with just a few simple steps.


7. The most important step you can take to protect yourself is to make sure that only you can use your devices and your accounts.

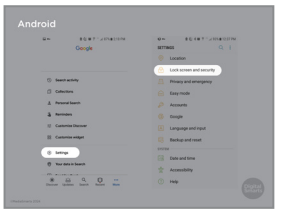

8. Phones, tablets and some computers are usually locked with a PIN. That's a code – usually numbers – that you have to enter to use the device.

   Most devices, though, aren't PIN-locked unless you turn that on. That should be one of the first things you do when you get a new device, or else anyone who picks it up can see and potentially access anything that's on it.

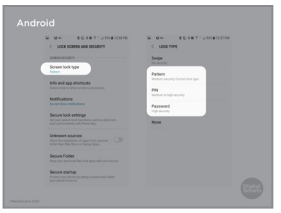



9. Next, let's see how to set up a PIN.

   On Apple devices like iPhones, tap Settings and then "Face ID and Passcode." ("Passcode" is their word for PIN.) It'll ask you to set a PIN with six numbers, but you can also choose to do a shorter one or one that includes letters.



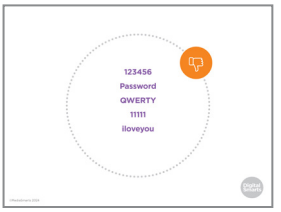

10. On Android devices, tap Settings and then scroll down to "Lock Screen and Security."




**11.** Then tap “Screen Lock Type”,

And then pick the type of lock you want – a PIN, a password, or a pattern that you draw on the screen.

It doesn’t matter too much which one of those you choose, so long as you lock your device in some way. If possible, hold your device so nobody can see you enter your password, PIN, or pattern.




**12.** Unlike devices, if you want to use email or social networks like Facebook, you’ll need to make a password.

A lot of people use passwords that aren’t safe because they don’t have a lot of time to think of a password.

Here are some of the most common passwords:

123456

Password

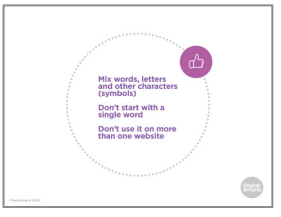
QWERTY (that’s the first six keys on the top row of a keyboard)

11111

Iloveyou

Other times, people use passwords that anybody who knows you can guess – your middle name or your date of birth, for example.

**13.** There are three common ways that people’s passwords are compromised: first, by using the *dictionary* or *brute-force* method, where a computer program guesses either every word in the dictionary or every possible combination or letters and numbers; second, guessing your password recovery questions, like your first pet’s name; and third, hacking the site or app itself and getting the passwords for *every* user there – or buying those passwords from someone else that hacked the site.




**14.** 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 just one thing – it's not just numbers and not just letters. Second, it isn't based on a single word.

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


**15.** After trying the most common passwords, most would-be "hackers" (people who break into other people's systems or accounts) use a program that tries every possible password. Because they're computer programs, they can do this very quickly. Having a mix of letters, numbers and other things like punctuation marks can slow that down a lot.

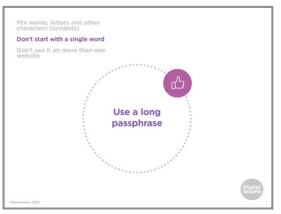
You can start with a regular word and replace some of the letters with numbers or other characters, like what is on this slide.

If you can, use a mix of upper and lower-case (small and capital) letters as well. Don't always put the capital letter at the beginning!

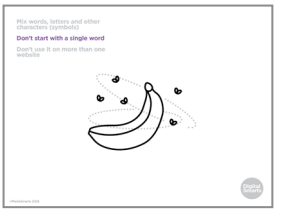

**16.** Programs that try to guess passwords often run through the whole dictionary, so even if you've changed a few letters into numbers or characters they can still guess it.

To help with that, make a pass *phrase* with your word – turn "bananas" into "bananas are yellow" or "I like bananas," for example. (Most passwords don't allow spaces, so you'll just keep the words together.)

Then replace some letters in the new words with numbers or other characters.




**17.** The longer a passphrase is, the harder it is to crack using a dictionary attack or the brute- force method.




**18.** If you can, choose a long passphrase that is easy to picture in your mind. To remember "fruit flies like a banana," for instance, you might imagine this picture.


**19.** Finally, you don't want to use the same password on more than one site. Remember, a lot of the time it's the sites themselves that get hacked, not people's accounts, so hackers can get at even a strong password.

The problem is remembering different passwords for different sites. One easy way to do that is just to add the first and last letter of the site to the password. For example, for your Facebook account you'd put F before the password and K after. For your Kijiji account you'd put K before the password and I after.

You don't have to use this method exactly. You can put the letters in the middle, or reverse them, or whatever you like, so long as it's a pattern you'll remember.


**20.** You can use this method for every password *except* for your email. Because you use your email address to sign up for most of your other accounts, it's the one that is the most important to keep private. You can use the same method to come up with a password, but make sure it's a totally different one from all your other accounts.

You still only need to remember two passwords – the one that you use for your email address, and the other one that you change slightly for each of your other accounts.

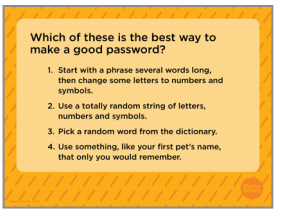

**21.** Another option is to use a *password manager*. This is a program that you use to handle your passwords for different accounts. It creates a different, almost unbreakable password for each account and then handles logging in to the accounts for you.

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

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 it can log into all of your accounts.


**22.** If you want to know more about password managers, you can check this article at Get Cyber Safe. Just enter the link at the bottom of the screen – tiny.cc/pm4u – in the address bar of your browser, or do a search for "How to choose the right password manager for you."


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

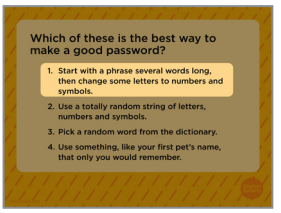



**24.** Which of these is the best way to make a good password?

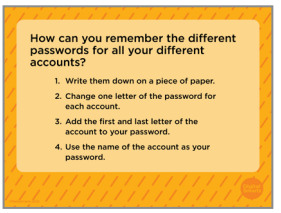
To start with a phrase and change some letters to numbers and symbols? To use a totally random string of letters, numbers and symbols?

To pick a random word from the dictionary?

Or to use something, like your first pet's name, that only you would remember?




**25.** The best approach is to make a *pass phrase* – a phrase several words long – and then change some of those letters to numbers and symbols. That way it's hard to guess but easy to remember.




**26.** How can you remember the different passwords for all your different accounts? Write them down on a piece of paper?

Change one letter for each account?

Add the first and last letter of the account to your password? Or use the name of the account as your password?


**27.** Remember, the most important thing is to *not* use the same password for more than one account. Adding the first and last letter of the account (like "F" and "K" for Facebook) helps you make it unique but is easy to remember.


**28.** Why should you use a completely different password for your email account? Is it because it's where your most private things are?

Because it's how other accounts reset your password if you forget it? Because email accounts have weaker security?

Or because a stronger password will keep you from getting spam emails?


**29.** Usually, when you forget a password you can send a *recovery question* to your email address. That means someone who has access to your email address might be able to access a lot of your other accounts.


**30.** What does a password manager do?

Does it help you remember your passwords? Or come up with passwords?

Does it make and remember strong passwords for you? Or change your password every month?


**31.** Password managers make strong passwords for you, remember and enter them automatically them. (Of course, you need a good password for your password manager!)


**32.** Let's try making some good passwords.

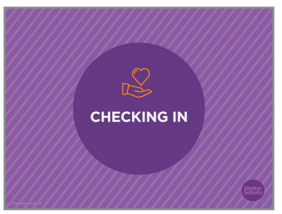
Think of a word and write it down on the Password Builder worksheet.


**33.** Start with a regular word that's at least six letters long, like "bananas." Replace some of the letters with numbers and symbols, like "6@n@n@s." Make a phrase with the word, like "ilike6@n@n@s."

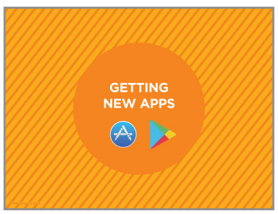
Replace some of the new letters, like "!l!ke6@n@n@s."

Add the first and last letter of the account the password is for, like "f!l!ke6@n@n@s" (for Facebook).

Now turn the page over and see if you can remember it later!




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




**35.** Most computers, smartphones and tablets come with a lot of apps already installed, but you may want to get new ones. Someone in your family may be using a new social network like Instagram that you want to join, for example, or there may be a new game that your kids want to play.


**36.** An app is a program that you can use on a phone or tablet. A lot of things that you would do through a browser on a computer, like watching Netflix or using a social network like Facebook, you can usually do with an app on a phone or tablet.

To use an app that's not already on your device you have to *download* it. That means you make a copy of it on your device.

You can also download other things like photos, videos or music files. Those can come from websites, from texts or emails, or other kinds of messages that people send you.


**37.** Because downloading puts something new on your computer, it can be risky. If something you download isn't what you think it is, you might end up letting someone put malware on your computer.

Malware are programs that make your device do things you don't want it to do. Some kinds of malware are computer viruses, which use your computer to send copies of themselves to other computers, and spyware, which watches what you do online and sends that information to the people who made it. These programs can let them get into things like your bank account or other online accounts.

To be safe, never download anything from an email, text or other message that you didn't ask for.

When you're using a browser, only download from websites you trust.

You should also make sure the web address starts with h t tp s (watch for the "s" at the end) and has this padlock symbol in the address bar. That doesn't necessarily mean that a site is trustworthy – but it *does* mean that nobody else can see what you send to the site or what the site sends to you.


**38.** When you're using a phone or tablet, make sure to only download apps from the official store. For Apple devices like iPhones that means the App Store. Apps for Android devices should be downloaded from the Play Store.

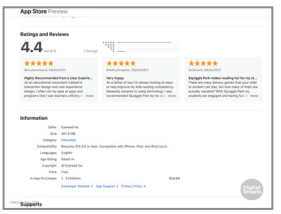
Your device should come with one of those apps already on it.

If you hear about an app, go to the App Store or Play Store and search for it there.

Remember that a lot of apps don't cost anything to download but you may have to pay to get the full version. Some others make you watch ads to use them or try to get you to buy extra things while you're using them. Make sure to read what it says on the store page for that app about costs and payments.

You may have to give your credit card information when you start an App Store or Play Store account. You shouldn't be charged for anything unless you buy an app, or unless you buy something inside an app.

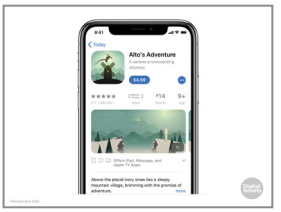
To be safe, don't download apps while using public WiFi, like at a library or coffee shop. Because they're used by many people, there are ways to intercept what you're sending and receiving.




**39.** Both app stores also let users rate apps, so you can check out what other people have said about an app, too.

**40.** Let's walk through downloading an app. On an iPhone or iPad, tap the App Store icon on your screen to start.

If you haven't used it before, you'll need to make an App Store account.

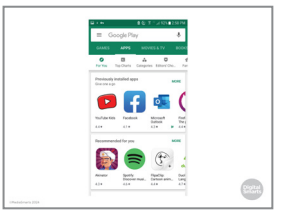



**41.** Now you can search for the app. You might look for the app or for what you want the app to do. (For example, you might type "weather" to find a weather app.)

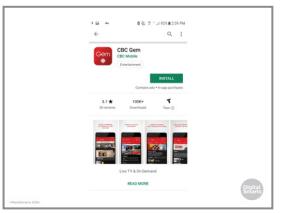
When you see the different choices, tap on whichever one interests you.

Now you'll see information about the app. If it's free you can download it by tapping: Get. If it costs money, tap on the price. After that you'll need to confirm that you want to buy it.

Once the app has downloaded, it will have its own symbol on your home screen.




**42.** In the Google Play Store you can either search for a specific app or browse by topic.




**43.** Now tap on any app that interests you. If you decide to download it you can tap Install if it's free or tap the price if it costs money.

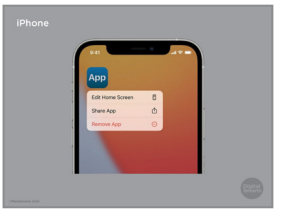
An icon for it will appear on the last page on your phone.


**44.** Some apps look safe at first, but ask you to give them personal details that they don't need. Don't enter personal information that the app doesn't need to work and uninstall (remove) an app that makes you do that to use it.

If an app asks you to let it do something strange with your phone, like make phone calls or use your camera when there's no good reason for it to, say no and uninstall it.


**45.** To uninstall apps from an Android device, touch the app's icon and hold your finger on it until the Uninstall option appears. Tap it to uninstall.

On an iPhone, tap and press the icon until an X appears at the upper left corner. Tap the X and then tap Delete in the new window that appears.




**46.** (On the most recent iPhones, the Remove App option will appear any time you touch and hold an app's icon.)


**47.** Another thing to watch out for with apps is how much data they use. Data is what lets you use the internet on your smartphone and costs money to use.

If you only use WiFi that's not as big a deal.

If you use data, though, it may cost you money if you go over your limit set in your cellphone plan. A lot of apps also use data when they're on, by sending video, photos, music, and so on. Even a weather app will send and receive data to tell the app where you are and to send information about the weather to your device. Apps can also use data in the background, even if you're not using them.

To see how much data you're using on either an Apple or Android device, start by tapping Settings. On an iPhone or iPad tap Cellular next. From here you can set certain apps to not use data unless you approve it by sliding any of these switches to the left.

On an Android device, tap Data Usage. From there you can turn data on or off and set it to let you know any time an app wants to use data.

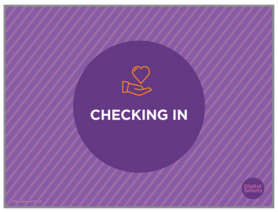

**48.** Let's try finding some apps that will help you do useful things.

If you're using a phone or tablet, open the Play Store or App Store. If you're using a Windows computer, go to the Microsoft store (the first web address on the screen). If you're using a Chromebook go to the Chrome web store (the second web address on the screen.)

Now see if you can find three apps that you might like to use:
An app for your local public library.

An app that will give you a weather forecast.

And an app that will help you plan meals for yourself or your family.




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


**50.** Another thing that worries a lot of people when they go online is getting caught by scams. By "scams" I mean when people try to trick you into giving them money or your personal information.

There are a lot of scams out there, and they can cost you a lot of money.

Luckily, knowing what to watch out for can help you spot almost any online scam.

**51.** There are two main things that scammers try to get from you. Either they want you to send them money, or they want your personal information. A lot of times they'll want you to send your bank account or credit card information so they can get money from you, or your password to your email or social network accounts so that they can pretend to be you.

**52.** Scams can come to you in different ways.

A lot of them come through email – so be suspicious of email that comes from someone you don't know. The same is true of text messages or messages on social networks like Instagram.

Sometimes, though, scammers will pretend to be someone you do know. Someone you know might also have downloaded malware that makes their computer send fake messages.

One popular scam that takes advantage of this is when you get a message from someone you know saying that they are in trouble and need money right away. **Don't** answer these messages – if you think the person you know might really be in trouble, contact them another way to find out.


**53.** Scammers also sometimes pretend to be places where you have an account, like your bank, your internet provider or your email provider.

Some of the signs that a message is a scam are if they're asking you to send any of that kind of information, if they're asking you to follow a link (that leads from one website to another) rather than go to their website on your own, or if they're trying to scare you by suggesting that you owe money or that one of your accounts is about to be closed.

Don't ever click on a link that's inside a message from a bank, Revenue Canada, your internet provider, email provider, or anyone else like that.

Instead, enter the correct web address into the address bar and check there. You can also get the correct phone number – check your bill, or go to the correct web address – and call them on the phone to find out if there really is a problem.


**54.** Sometimes scammers try to trick you by making you think they will give *you* money. You might get a message telling you that you have a tax refund, that you've won the lottery, or that you might be able to be part of a business deal.

As you can see from this example, while typos and bad grammar should still make you suspicious, you can't count on scam emails having them.

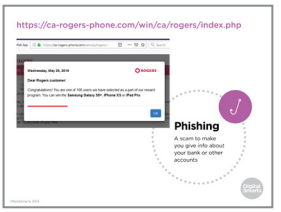
CRA will never email or text a link, or ask you for personal information through email or text. They will always direct you to log in and go to My Account "on the CRA webpage" without providing any links or web addresses.

Sometimes, like in the example here, they just want you to click on the link so that they can either get your personal information or download malware onto your computer.

Other times, there may be a file or document attached to the message. This can also contain malware, even if it seems like a regular document.

No matter what, remember that if something seems too good to be true, it probably is. If you get a message like this, just delete it.

If you think there's a chance it might be true, go to the real website or call them on the phone. (**Don't** use a phone number or web address from that message – look it up on your bill or on a search engine.)



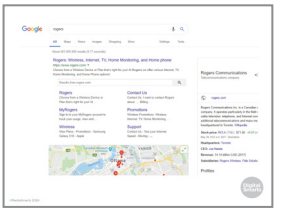

**55.** One of the most common types of scam is called “phishing.” That’s when the scammers are trying to get you to give them information about your bank accounts or other accounts.

Here’s an example of a recent scam that actually appears as a web page that opens without you trying to open it. As you can see, it’s an example of the “money for nothing” scam because it’s telling you that you can enter a draw to win a tablet or smartphone.

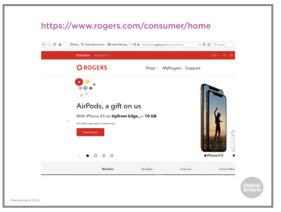
If you’re not actually a Rogers customer, then you already know it’s a scam. If you are, though, how can you find out?

First, you’ll want to look at the web address and you’ll see that it looks a bit strange. Not Rogers dot com or Rogers dot see eh (.ca), which you might expect, but see eh dash rogers dash phone dot com.


**56.** If you want to double-check, you can go to Google and do a search for Rogers (or look for the web address on one of your bills).

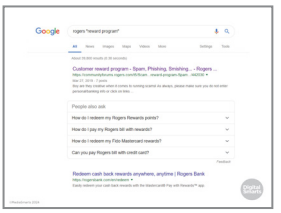


**57.** Now you’ll see that it is Rogers dot com, not the address you saw before.



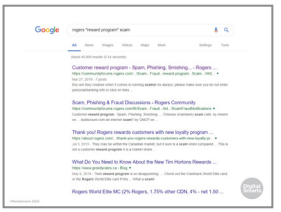

**58.** If you go to the real Rogers site, you’ll find that there’s nothing there about the contest.

Remember that on the internet it’s pretty easy to make a fake website that looks a lot like the real one, but it’s a lot harder to fake a web address.

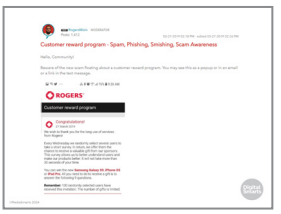


**59.** Another thing you can do is search for what the message is promising you.

If we do a search for Rogers and reward program, for example, the top result is a post warning us about the scam.




**60.** If we do the same search and add the word "scam" we get an even clearer message that this is a scam --



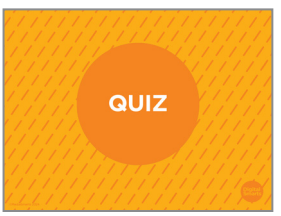

**61.** -- and if we follow one of those links we'll see a message from Rogers warning us about the scam.


**62.** One last kind of scam that doesn't directly involve money is *identity theft*. That's when somebody pretends to be you so they can register for online accounts or take out a credit card in your name.

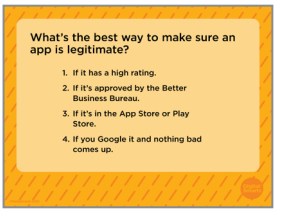
Identity theft usually happens because people have shared enough information about themselves that scammers who collect it can pretend to be them.

To keep that from happening, don't ever share any of these in a public space online, like a social network post:

- 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

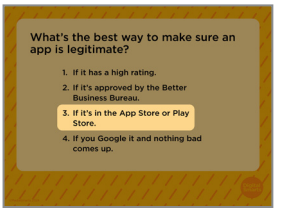



**63.** Let's do another quick quiz to review what we've learned in the last section.




**64.** What's the best way to make sure an app is legitimate?

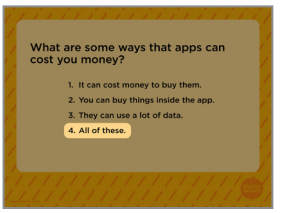
Is it if it has a high rating? If it's approved by the Better Business Bureau? If it's in the App Store or Play Store? Or if you Google it and nothing bad comes up?




**65.** Legitimate apps should be in the App Store (for an iPhone) or Play Store (for an Android device.)


**66.** What are some ways that apps can cost you money?

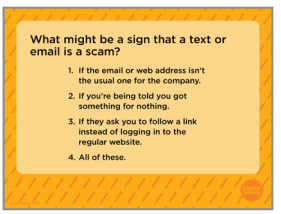
Because it costs money to buy them? Because you can buy things *in* them? Because they can use a lot of data? Or all of those?




**67.** All three of those are ways that apps can cost you money.


**68.** What is a phishing scam? Is it when people try to get you to send them money? When people try to get access to your bank or credit card accounts? When someone else pretends to be you? Or when someone tries to sell you something that isn't real?

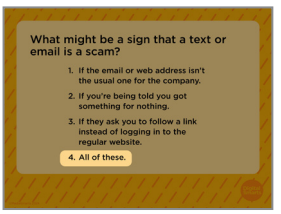

**69.** "Phishing" is when people try to get access to your bank or credit card accounts, usually by getting your personal information or by getting you to log in to a fake website.



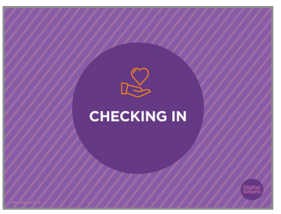

**70.** What might be a sign that a text or email is a scam?

Is it if the email or web address isn't the usual one for the company? If you're being told you got something for nothing?

If they ask you to follow a link instead of logging in to the regular website? Or all of these?




**71.** All of those are signs that a text or email is a scam.

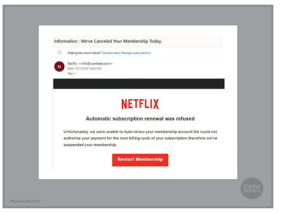



**72.** Before we go on, let's pause for a moment to see if anybody wants to take a break or needs any support.


**73.** Now let's take a look at the worksheet "Spot the Signs of a Scam."


**74.** They don't use your name; it's sent to the wrong email; or they don't have the right email address. (Sometimes it might *look* like the right address, but if you hover over it, it will look different.)


**75.** They want you to open an attachment or download a file; they want you to follow a link to log in; they want you to send them your login or personal information; and they want to scare you into doing something right away.




**76.** Now let's see if we can spot the signs that this email is a scam.

[Get feedback from participants – if they spot all of the signs, there's no need to read the text below.]

First, you can see that the email is designed to make you scared that your subscription is about to be canceled. That isn't a sure sign by itself – they would send you an email if that was going to happen – but it's a reason to be suspicious, especially if you don't have any reason to think there's a problem.

Next, look at the "From" address: an email from Netflix should come from an address that ends in Netflix.com. This one – from info@ixambee.com – looks like a scam.

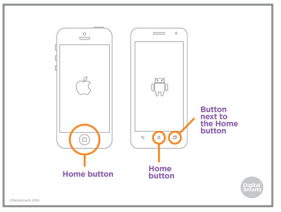
Finally, you can see that big "Restart Membership" button they want you to click on. That won't take you to Netflix, but to a website that wants to get your credit card info.


**77.** Now, remember that password you came up with a little while ago? Take a minute to see if you can remember it.

Now turn the paper over and see if you were right.


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

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

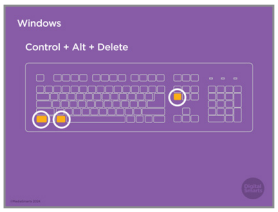



**79.** On phones and tablets you can usually exit an app without closing it by pressing the Home button.

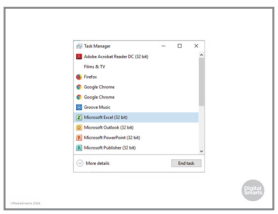
If you want to close an app on the iPhone or iPad, push the Home button twice. Then use your finger to swipe the app you want to close off the screen.

If you have a more recent iPhone or iPad with no home button, swipe your 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.

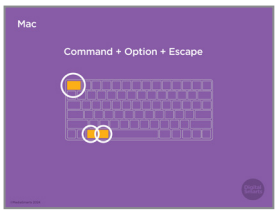
On an Android device, tap the square *next* to the home button, then swipe the app off the screen. (Sometimes this is on the right, sometimes on the left.)




**80.** If you're using a computer that uses the Windows OS, press the Control, Alt, and Delete buttons at the same time. (They may not be in exactly the same spots on your keyboard.)



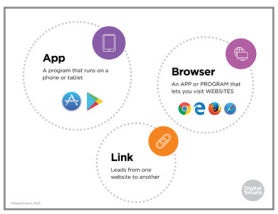
**81.** That will bring up this Task Manager window. Click on the program that you want to close and press End task.




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


**83.** If you have a problem that keeps happening, you can contact the support service for your device.

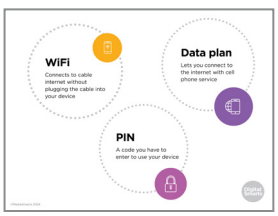
Here are the web addresses for the most common kinds of devices.




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

An *app is* something on a mobile device, like a phone or a tablet, that lets you do a particular job. Some examples of apps are games, email programs, or apps that let you watch YouTube or Netflix.

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




**85.** A *data plan* brings internet signals using cell phone signals.

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

A PIN is a code that you need to enter to use your device.

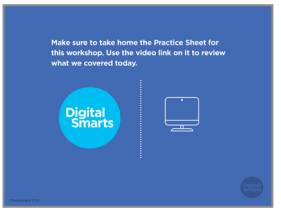

**86.** *Downloading* something means copying it from a website or email to your device.

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

A *phishing* scam is one where somebody tries to get you to give up some personal information, often about your bank accounts.


**87.** 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.



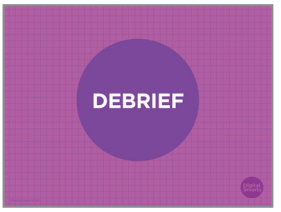

**88.** Make sure to take home the Practice Sheet for this workshop. Use the video link on it to review what we covered today.


**89.** 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.


**90.** 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.




**91.** 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?