Digital Smarts

Workshop Script

Discover Online Safety

Media Smarts

Digital Smarts

©MediaSmarts 2019

With funding from Canada

Media Smarts

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

Discover Online Safety

©MediaSmarts 2019

1. Welcome to our session on discovering online safety.

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.

What are some things you would like to do?

What are some things that you wish you could do?

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

What about the internet makes you nervous?

©MediaSmarts 2019

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

You don't have to answer out loud. Just think about these questions–

What are some things you like to do?

What are some things that you wish you could do?

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

©MediaSmarts 2019

3. 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 get government services or apply for a job.

But a lot of people are nervous about using the internet. There are things to be careful about: identify theft, computer viruses, scams and other problems.

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

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

Make a good password

Get new apps safely

Spot online scams

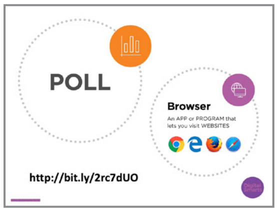
©MediaSmarts 2019

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

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.



POLL

Browser

An APP or PROGRAM that lets you visit WEBSITES

http://bit.ly/2rc7dUO

5. 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. A browser is an app or program that lets you visit web pages.

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 these browser symbols 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.

PASSWORDS AND PINS

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

PIN

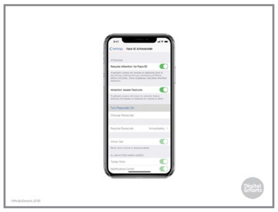
A code you have to enter to use your device

©MediaSmarts 2019

7. 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.

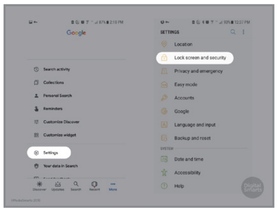
Most devices, though, aren't PIN-locked unless you turn that on. That should be one of the first things you do when you get a new device, or anyone who picks it up can see anything that's on it.

How many people here already use some kind of PIN-lock for their devices?

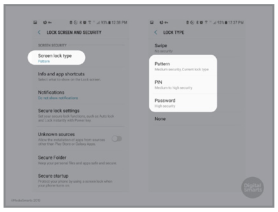


©MediaSmarts 2019

8. 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.



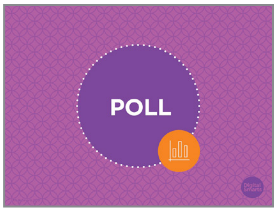
9. On Android devices, tap Settings and then scroll down to "Lock Screen and Security."


LOCK SCREEN AND SECURITY
SCREEN SECURITY
Screen lock type
Pattern
Info and app shortcuts
Select what to show on the Lock screen.
Notifications
Do not show notifications
Secure lock settings
Set your secure lock functions, such as Auto lock and Lock instantly with Power key.
Unknown sources
Allow the installation of apps from sources other than Play Store or Galaxy Apps.
Secure Folder
Keep your personal files and apps safe and secure.
Secure startup
Protect your phone by using a screen lock when your phone turns on.
LOCK TYPE
Swipe
No security
Pattern
Medium security, Current lock type
PIN
Medium to high security
Password
High security
None
Digital Smarts
©MediaSmarts 2019

10. 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.

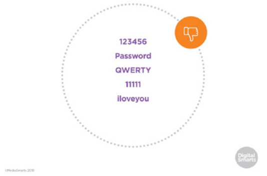
It doesn't matter too much which one of those you choose, so long as you lock your device in some way.



11. Now let's talk about passwords.

How many people feel like they know what makes a password good or bad?

How many people have trouble thinking of passwords for different accounts? How many people have trouble remembering passwords?



123456
Password
QWERTY
11111
Iloveyou

Digital Smarts
©MediaSmarts 2019

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

Because of that, you sometimes don't have a lot of time to think of a password. That's why a lot of people use passwords that aren't safe.

Here are some of the most common passwords used in 2018:

123456

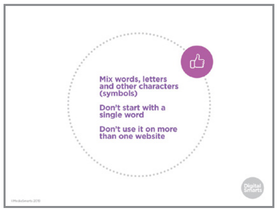
Password

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.



Mix words, letters and other characters (symbols)

Don't start with a single word

Don't use it on more than one website

©MediaSmarts 2019

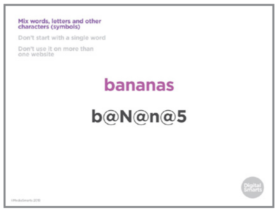
13. But even if you're not using one of the most common passwords, and your password isn't something that people could easily guess, there is a difference between weak and strong passwords.

What makes a password strong comes down to three things.

First, it isn't just one thing – just numbers or just letters.

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

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



Mix words, letters and other characters (symbols)

Don't start with a single word

Don't use it on more than one website

bananas

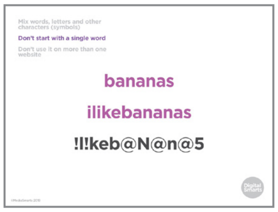
b@N@n@5

©MediaSmarts 2019

14. 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 here.

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!



Mix words, letters and other characters (symbols)

Don't start with a single word

Don't use it on more than one website

bananas

ilikebananas

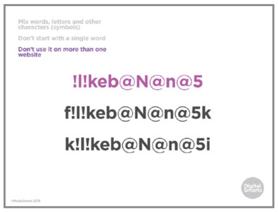
!l!keb@N@n@5

©MediaSmarts 2019

15. 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 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.



Mix words, letters and other characters (symbols)

Don't start with a single word

Don't use it on more than one website

!l!keb@N@n@5

f!l!keb@N@n@5k

k!l!keb@N@n@5i

©MediaSmarts 2019

16. Finally, you don't want to use the same password on more than one site. A lot of the time it's 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.

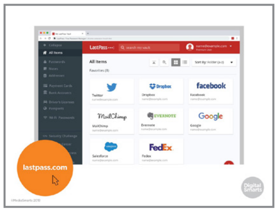
For your Kijiji account you'd put K before the password and I after.

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.

Use a totally different password for your email account

17. 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.



lastpass.com

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

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

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.

QUIZ

http://bit.ly/3326rqY

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

It'll work the same way as the poll you did a few minutes ago.

TRY THIS!

Make a strong password you can remember

20. Let’s try making some good passwords.

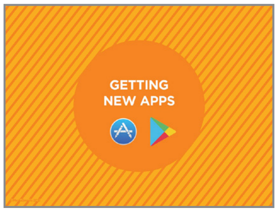
Think of a word and write it down on the Password Builder worksheet.

Now replace some of the letters with numbers or other characters.

Now make a phrase with the word, and change around some of the new letters.

I’ll come around and help anyone who’s having problems.

Now turn the paper over. We’ll check back in a little bit to see if you can remember it!



GETTING NEW APPS

21. 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.

App

A program that runs on a phone or tablet

Download

Copy something from a website to your device

©MediaSmarts 2019

22. 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 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.

Malware

Programs that make your device do things you don’t want it to

https://www.google.ca

©MediaSmarts 2019

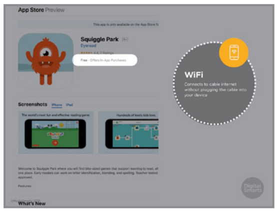
23. Because downloading puts something new on your computer, it can be risky. If something you download isn’t what you think it is, you might end up letting someone put malware on your computer.

Malware means 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. That 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 know you can trust.

You should also make sure the web address starts with h t t p s (watch for the "s" at the end) and has this padlock symbol in the address bar. That means that nobody else can see what you send to the site or that the site sends to you.



App Store Preview

This app is only available on the App Store fo

Squiggle Park 4+

Eyeread

★★★★★ 4.4, 7 Ratings

Free · Offers In-App Purchases

Screenshots iPhone iPad

The world's most fun and effective reading game.

Hundreds of levels kids love.

Welcome to Squiggle Park where you will find bite-sized games that support learning to read, all one place. Early readers can work on letter identification, blending, and spelling. Teacher tested approved.

Features:

What's New

WiFi

Connects to cable internet without plugging the cable into your device

24. 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.

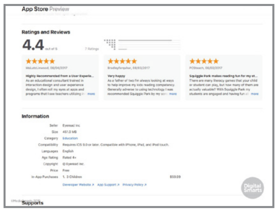
Your device should come with one of those apps already on it.

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.



App Store Preview

Ratings and Reviews

4.4 out of 5 7 Ratings

★★★★★ McLutzLinwood, 08/04/2017
Highly Recommended from a User Experie...
As an educational consultant trained in interaction design and user experience design, I often roll my eyes at apps and programs that I see teachers utilizing in more

★★★★★ Bradleyfarquhar, 08/03/2017
Very happy
As a father of two I'm always looking at ways to help improve my kids reading competency. Generally adverse to using technology I was recommended Squiggle Park by my son more

★★★★★ PCSteach, 08/02/2017
Squiggle Park makes reading fun for my st...
There are many literacy games that your child or student can play, but how many of them are actually valuable? With Squiggle Park my students are engaged and having fun all more

Information

Seller	Eyeread Inc
Size	451.0 MB
Category	Education
Compatibility	Requires iOS 9.0 or later. Compatible with iPhone, iPad, and iPod touch.
Languages	English
Age Rating	Rated 4+
Copyright	© Eyeread Inc.
Price	Free
In-App Purchases	1. 3 Children $59.99

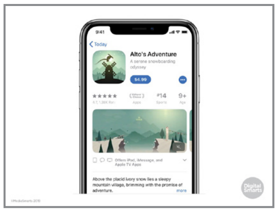
Developer Website ↗ App Support ↗ Privacy Policy ↗

Supports

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

26. 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.

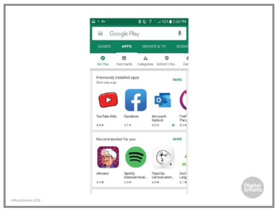


27. Now you can search for the app. You might look for the app or for what you want the app to do. (For example, you might type “weather” to find a weather app.

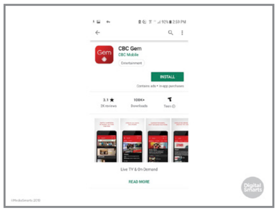
When you see the different choices, tap on whichever one interests you.

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.



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



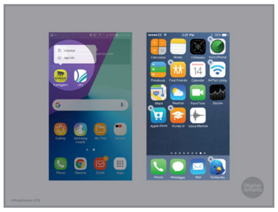
29. Now tap on any app that interests you. If you decide to download it you can tap Install if it’s free, or tap the price if it costs money.

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

CAUTION!

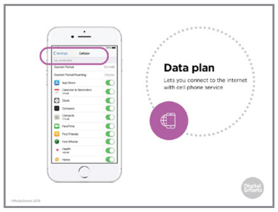
30. Some apps look safe at first, but ask you to give them personal details that they don’t need. Don’t enter personal information that the app doesn’t need to work, and uninstall (remove) an app that makes you do that to use it.

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.



31. 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. (On the most recent iPhones, the Delete App option will appear any time you touch and hold an app’s icon.)



Data plan

Lets you connect to the internet with cell phone service

32. 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 – though things like videos can still make you go past your data limit.

If you use data, though, it will cost you money when you download an app and any time that app updates. 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.

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.

QUIZ

http://bit.ly/2CZtuI7

Digital Smarts

33. Let's do another quick quiz to make sure you caught all that.

TRY THIS!

Library
Weather
Menu Planning

https://www.microsoft.com/store/apps
https://chrome.google.com/webstore/category/apps

Digital Smarts

34. 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 web address at the top). If you're using a Chromebook go to the Chrome web store.

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.

I'll come around and help anyone who's having problems.

Now turn to the person next to you and talk about your experience. How easy was it? How many different choices did you have for each app? What could you learn about each app that might help you decide if it was right for you?

35. 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 if you believe them.

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

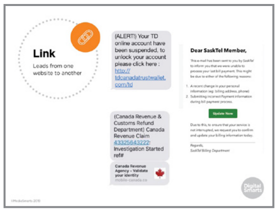
36. There are two main things that scammers try to get from you. Either they want you to send them money, or they want your personal information. A lot of times they'll want you to send your bank account or credit card information so they can get money from you, or your password to your email or social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

37. 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 Twitter.

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.



(ALERT!) Your TD online account have been suspended, to unlock your account please click here : http://tdcanadatrustwallet.com/td

(Canada Revenue & Customs Refund Department) Canada Revenue Claim 43325643222: Investigation Started ref#

Canada Revenue Agency - Validate your identity
mobile-canada.co

Dear SaskTel Member,

This e-mail has been sent to you by SaskTel to inform you that we were unable to process your last bill payment. This might be due to either of the following reasons:

1. A recent change in your personal information (eg: billing address, phone)
2. Submitting incorrect Payment information during bill payment process.

Due to this, to ensure that your service is not interrupted, we request you to confirm and update your billing information today.

Regards,
SaskTel Billing Department

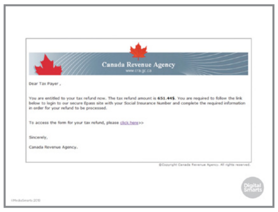
©MediaSmarts 2019

38. Scammers also sometimes pretend to be places where you have an account, like your bank or your internet 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 or anyone else like that.

Instead, go to the real website and check there, or call them on the phone to find out if there really is a problem.


Canada Revenue Agency
www.cra.gc.ca

Dear Tax Payer ,

You are entitled to your tax refund now. The tax refund amount is **651.44$**. You are required to follow the link below to login to our secure Epass site with your Social Insurance Number and complete the required information in order for your refund to be processed.

To access the form for your tax refund, please click here>>

Sincerely,

Canada Revenue Agency.

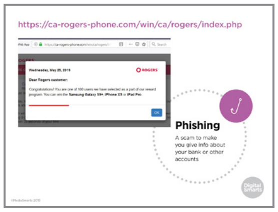
©Copyright Canada Revenue Agency. All rights reserved.

39. 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.

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.

No matter what, remember that “there’s no such thing as a free lunch.” 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.)


https://ca-rogers-phone.com/win/ca/rogers/index.php

Wednesday, May 29, 2019

Dear Rogers customer:

Congratulations! You are one of 100 users we have selected as a part of our reward program. You can win the **Samsung Galaxy S9+**, **iPhone XS** or **iPad Pro**.

Phishing

A scam to make you give info about your bank or other accounts

40. 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.

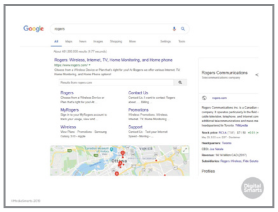
If you’re not actually a Rogers customer then you already know it’s a scam. If you are, though, how can you find out?

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

rogers

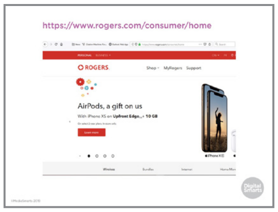
rogers
rogers **yahoo**
rogers **internet**
rogers **login**
rogers **anyplace tv**
rogers **bank**
rogers **contact**
rogers **centre**
rogers **tv**
rogers **wireless**

41. 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).



Rogers: Wireless, Internet, TV, Home Monitoring, and Home phone

42. Now you'll see that it is Rogers dot com, not the address you saw before.



https://www.rogers.com/consumer/home

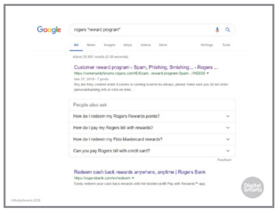
ROGERS

AirPods, a gift on us

With iPhone XS on Upfront Edge + 10 GB

43. 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.

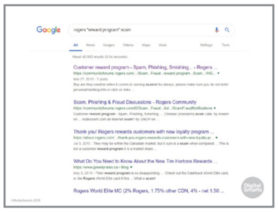


rogers "reward program"

Customer reward program - Spam, Phishing, Smishing, - Rogers ...

44. Another thing you can do is to 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.

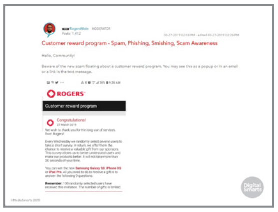


rogers "reward program" scam

Customer reward program - Spam, Phishing, Smishing, - Rogers ...

Scam, Phishing & Fraud Discussions - Rogers Community

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



Customer reward program - Spam, Phishing, Smishing, Scam Awareness

ROGERS

Customer reward program

Remember: 100 randomly selected users have received this invitation. The number of gifts is limited.

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

NEVER share:

- Full name
- Full date of birth
- Social Insurance Number
- Mother's maiden name
- Credit card information
- Driver's licence or passport number

47. 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

TRY THIS!

Spot the signs of a scam

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

[Read the first page of the worksheet.]

Take a look at the email on the second page and see how many of those signs you can find.

Now turn to the person next to you and compare notes. Did you find the same things?

TRY THIS!

Let's take a look at those five signs.

49. Let's take a look at those signs.

[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.

TRY THIS!

Make a strong password you can remember

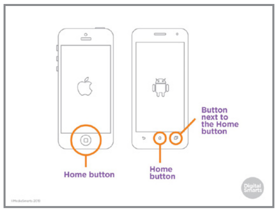
50. Now, remember that password you came up with a little while ago? Take a minute to see if you *can* remember it.

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

What if something goes wrong?

51. 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.

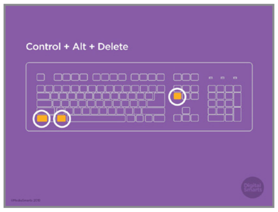


52. On phones and tablets you can usually exit an app without closing it by pressing the Home button.

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.

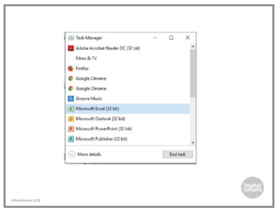
If you have a more recent iPhone or iPad with no home button, swipe young finger halfway up from the bottom of the screen and then lift your finger. This will open a new window where you can close apps.

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.)



Control + Alt + Delete

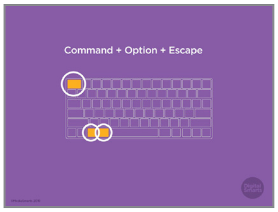
53. If you're using a computer that uses the Windows OS, press the Control, Alt and Delete buttons at the same time. (They may not be in exactly the same spots on your keyboard.)



Task Manager

- Adobe Acrobat Reader DC (32 bit)
- Films & TV
- Firefox
- Google Chrome
- Google Chrome
- Groove Music
- Microsoft Excel (32 bit)
- Microsoft Outlook (32 bit)
- Microsoft PowerPoint (32 bit)
- Microsoft Publisher (32 bit)

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



Command + Option + Escape

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

support.apple.com

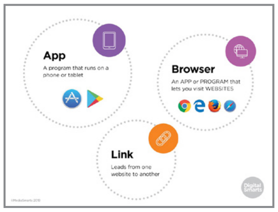
support.google.com

microsoft.com/windows

©MediaSmarts 2019

56. 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.



App
A program that runs on a phone or tablet

Browser
An APP or PROGRAM that lets you visit WEBSITES

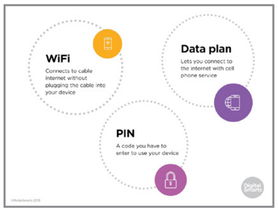
Link
Leads from one website to another

©MediaSmarts 2019

57. 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.



WiFi
Connects to cable internet without plugging the cable into your device

Data plan
Lets you connect to the internet with cell phone service

PIN
A code you have to enter to use your device

©MediaSmarts 2019

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

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.

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

Download
Copy something from a website to your device

Phishing
A scam to make you give info about your bank or other accounts

Malware
Programs that make your device do things you don't want it to

©MediaSmarts 2019

59. *Downloading* something means copying it from a website or email to your computer.

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.

QUESTIONS?

60. 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.

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

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

POLL

http://bit.ly/2KF4rP8

62. 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.