# Let’s talk about Online privacy

## Description

Find out how to protect your online privacy when using the Internet in this discussion-based class. Explore topics such as metadata collection, online tracking, identity theft and more. Register by phone for this or other classes in the Internet Essentials series. Each class must be registered for separately.

## Learning Goals and OUTCOMES

**Digital Proficiency** > Secure > Secure Private Information

*Learners will be able to…*

* Choose secure and memorable passwords
* Identify, select and manage support services for account management as needed (e.g. password managers)
* Recognize and critique government and corporate digital surveillance, the motivations and the basic legal issues involved
* Recognize digital crimes

**Digital Proficiency** > Secure > Secure Digital Devices & Services

*Learners will be able to…*

* Identify and apply web browser privacy features

**Digital Proficiency** > Secure > Understand & Shape Online Identity

*Learners will be able to…*

* Identify sensitive digital information for security purposes in personal and professional contexts
* Examine and assess the consequences of sharing data online

## Preparation

|  |  |
| --- | --- |
| Equipment Needed: | * Projector/laptop * Internet access, Sound |
| **Materials Needed:** | * See *Digital Literacy Preparation, Setup & Closing Checklist* for full preparation details. Find the checklist here: <https://hub.vpl.ca/content/86022> * PowerPoint on USB * Handouts for learners * Evaluation forms for learners * Blank certificates |
| **Setup Procedures:** | * Review the “Adult Teaching & Learning at VPL” teaching philosophy * Review the lesson materials * Confirm that all necessary space and equipment has been booked |
| **Background Reading** | * <https://securityinabox.org/en/> (security tools for devices and browsers) * <http://www.ghacks.net/2015/12/28/the-ultimate-online-privacy-test-resource-list/> (links to websites that test various privacy settings) * <https://securityinabox.org/en/guide/social-networking/web/> (privacy settings on a few popular social networks) * <https://www.eff.org/https-everywhere> (a Firefox, Chrome, and Opera extension that encrypts your communications with many major websites) * <https://privacyplan.ca/recommendations/end-mass-surveillance> (government metadata collection and surveillance) * <https://www.mozilla.org/en-US/teach/smarton/surveillance/> (government surveillance, with an even scarier video than the one on the Privacy Concerns: Government Surveillance slide) * <https://privacyinternational.org/node/53> (What is Metadata?) * <https://www.lullabot.com/articles/https-everywhere-security-is-not-just-for-banks> HTTPS Everywhere: Security is Not Just for Banks |
| **# of Staff Required and/or Staff: Learner Ratio** | * 1-12 learners: 1 instructor * For branch meeting room capacities, please see: <http://hub.vpl.ca/content/64490> |

## Opening

Before doors open:

* Write your name and [programs@vpl.ca](mailto:programs@vpl.ca) on the whiteboard (include phone number 604-331-3603 for more basic digital literacy classes)
* Distribute handouts, evaluation forms (if applicable)
* Test internet & speakers
* Turn the computers for learners on before class starts
* Open any relevant websites needed for lesson.

As learners enter

* Welcome learners

| **LEARNING ACTIVITIES** | | | | **LEARNING OUTCOMES** |
| --- | --- | --- | --- | --- |
| **Slide and/or Demo** | **Time** | **Trainer Does** | **Learners Do** |  |
|  | **5 min** | **INTRODUCTION**  *Welcome* students; *introduce* yourself; *introduce* the class and series  *Remind* learners of washroom locations; turn off cell phones; etc.  *Ask* if everyone can hear you. | * Listen to instructor * Respond to instructor’s prompts |  |
|  | **5 min** | * Come and **talk with me at the end of class if you have attended this series for the past two weeks** so I can get you your certificate. | * Listen to instructor * Ask questions |  |
|  | **5 min** | **LEARNING OPPORTUNTITIES AT VPL**   * There are several ways you can learn more about this topic. One way is through online learning at yourown pace.   **VPL Research Guides**  <https://www.vpl.ca/researchguides>   * Wide variety of topics; collected books & online resources   *Show* them how to find the Research Guides from the VPL website and how to **navigate to the Internet Essentials guide** | * Listen to instructor * Ask questions |  |
| H:\PLG\Privacy\privacyslideshow\Slide4.PNG | **2 min** | **LEARNING OPPORTUNITIES AT VPL**   * This is **one of the many learning opportunities** at the library. * Today’s class is meant to be an **introduction to the topic** – there are lots more ways to delve deeper. * There are many other ways to learn and **get help** on this and other topics at the library. * **Drop-in** to any branch * **Computer Practice Drop-In** at Central * **Call or email** the library | * Listen to instructor * Ask questions |  |
|  | **5 min** | **LEARNING OBJECTIVES**  ***Review* slide** and read learning outcomes listed on slide  ***Lead* a round** where people introduce themselves and answer this question:   * Please share **your name and what brings you here today.** What are you hoping to learn from this class?   ***Set* expectations.**   * We’re going to discuss different ways to protect your privacy online, including practical steps you can take to keep yourself safe from identity theft and corporate collection of your data | * Listen to instructor * Ask questions * Introduce self and what they hope to get out of the class |  |
| H:\PLG\Privacy\privacyslideshow\Slide6.PNG | **7 min** | **ONLINE PRIVACY**   * Together, we’re going to look at how and why we share information online.   *Ask:*   * In what ways do we share our data online?   Possible answers:   * + posting on **social media**   + signing up for **government services** (i.e. to receive benefits)   + providing **info to companies** in order to use their services (i.e. banking info & online shopping)   + When **shopping online** (i.e. providing a credit card, either stored or temporarily; providing a shipping address that can be saved for future purchases)   + **using apps** (i.e. **fitness trackers** which accumulate and store information)   + using **GPS (location services) on mobile devices** (i.e. using Google Maps, uploading photos to Instagram, using Bluetooth wireless accessories   + If we **staying logged in** (on a device or computer: i.e. Facebook or Google)   *Ask*   * **What are our reasons for sharing this information online?**   Possible answers:   * **Convenience** (staying logged in) * **Connection** (social media) * **Save money** (by shopping online) | * Discuss as a group how and why we share information online? | * Examine and assess the consequences of sharing data online |
|  | **3 min** | **REWARD AND RISK**  *Introduce* the **concept of risk versus reward**   * Just like in our offline lives, we **share information online because we get something out of it**, but there is always some **element of risk** involved (even if it’s usually very minor)   *Read and* ***discuss* example on slide**  *Emphasize*the **goal is to be informed about when you are giving away information** and how that information can be used; it’s **not that this is wrong,** it’s that it involves risk and that risk should be understood. | * Listen to trainer * Ask questions | * Examine and assess the consequences of sharing data online |
|  | **5 min** | **REASONS PEOPLE COLLECT YOUR DATA**  *Discuss* **who might want to collect data**, and what their **motivations** might be. ***Click* to reveal each new point** on slide.   * **Targeted advertising**   + Using information about your online behaviour, advertisers can figure out which ads you’re most likely to be interested in, or ensure that you keep seeing the same product advertised * **Selling data to advertisers**   + Browsers and search engines collect data, create a profile of you, which can be sold to advertisers * **Product development**   + Involves monitoring how you use a service so that the creators are able to improve service * **Malicious people** (phishing, identity fraud)   + More on this later in the presentation. * **Surveillance, public safety**   + Government and security agencies monitor internet traffic and scan for “red flag” behaviour   + They can also connect suspected individuals together through their online behaviour   + It is not legal for the government to “watch” you (eg read your emails or online conversations), but they *can* record who you are contacting and which sites you are visiting 🡪 think of it as sending a letter: they can’t read the letter, but they can read the envelope to see who you’re sending it to   If answers are all negative, *prompt* with “what are some positive reasons someone might want to gather data?” | * Discuss * Ask questions | * Recognize and critique government and corporate digital surveillance, the motivations and the basic legal issues involved * Examine and assess the consequences of sharing data online * Examine and assess the consequences of sharing data online |
| **H:\PLG\Privacy\privacyslideshow\Slide8.PNG** | **4 min** | **TRACKING**  ***Play* video** [2:19]  *Ask:*   * Any questions or comments about the video?   ***Review* any concepts** that learners have questions about. | * Watch video * Listen to trainer * Ask questions | Identify and apply web browser privacy features |
|  | **3 min** | **COOKIES**   * The previous video touched on cookies, but this next video goes into a bit **more depth** to explain what they are. * After this video we will talk about how to see and delete your cookies in your browser   ***Play* video** [end it at 1:40]  *Ask:*   * Any **questions or comments** about the video? | * Watch video * Listen to trainer * Ask questions | Identify and apply web browser privacy features |
|  | **5 min** | **HOW TO DELETE COOKIES**  ***Demonstrate* how to delete cookies in Firefox**. [Click the menu icon on the right, select Options 🡪 Privacy & Security 🡪 Scroll down to Cookies and Site Data 🡪Clear data.]  *Demonstrate* **how to view which cookies you have** with your browser by clicking on Manage Data. | * Follow along to clear cookies in browser | * Identify and apply web browser privacy features * Locate, review and modify important computer and device settings for security |
| **H:\PLG\Privacy\privacyslideshow\Slide10.PNG** | **8 min** | **HISTORY AND PRIVATE BROWSING**  ***Play* video** [1:46]  *Ask:*   * Any **questions or comments** about the video?   *Emphasize* that **private browsing & history doesn’t relate to how search engines and websites track your online activity**.  ***Demonstrate* how to open a private browser in** Firefox  [click “File” or the menu icon on the right, select “New Private Window”]. *Show* the **mask icon** that appear on the top right. | * Listen * Ask questions * Follow along with how to open a private browsing window | * Identify and apply web browser privacy features * Locate, review and modify important computer and device settings for security |
| **H:\PLG\Privacy\privacyslideshow\Slide11.PNG** | **8 min** | **BROWSER EXTENSIONS**  ***Explain* Browser Extensions**   * They are like **small mini-programs that you add to your browser** to provide additional features, such as blocking advertisements, finding shopping codes for discounts, extra security.   + - You **can pick and choose** which extensions to install onto your browser. Some examples we recommend adding to Firefox to increase your online privacy include (these are on the handout):     - **Privacy Badger** – stops advertisers and other third-party trackers from secretly tracking where you go on the web.     - **Disconnect.me –** anti-tracking, anti-cookie, block 3rd party tracking cookies     - **Ghostery** you decide what data you share with the trackers on the sites you visit. * **https://Everywhere:** protects your communications by enabling HTTPS encryption automatically on sites that are known to support it, even when you type URLs or follow links that omit the https: prefix.   ***Demonstrate* how to find add-ons in Firefox**   * Click the menu icon in the top right corner, and select “add-ons”. On the left menu bar, select “get add-ons”, then select “find more add-ons” and search “https everywhere”]   ***Point out* the “recommended” tag** from Firefox as a way to help people select good add-ons. | * Listen, ask questions * Follow along to add-ons | * Identify and apply web browser privacy features * Locate, review and modify important computer and device settings for security |
| **N6.png** | **7 min** | **IDENTITY THEFT AND FRAUD**  *Ask:*   * + **What is** **identity theft**?   *Answer:*   * + - When someone gathers enough information about you that they can impersonate you for illegal purposes.   *Ask:*   * + **What happens when those interested in using our information for fraudulent purposes gather enough information about us?**   *Possible answers:*   * + Access your bank accounts or open new ones   + Apply for loans, credit cards & goods and services   + Make purchases   + Hide criminal activities   + Obtain passports   + Receive government benefits * **What kind of information do you think is used for identity theft & fraud**?   *Possible answers:*   * + Full name, Address, Date of birth   + Social Insurance Number   + Mother's maiden name   + Usernames and passwords for online services   + Driver's license number, other ID numbers   + Personal identification numbers (PIN)   + Credit card information   + Bank account numbers   + Signature   *Explain* that often the information people are looking for is the **answer to your “security questions”**   * How might people gather this kind of information?   *Possible answers:*   * From our **social media posts**/comments * By **sending us fake emails** prompting us to login and input our personal information at fake sites (i.e. fake Paypal, eBay, bank, Apple store sites etc.). | * Listen to trainer * Ask questions | * Identify sensitive digital information for security purposes in personal and professional contexts * Recognize and critique government and corporate digital surveillance, the motivations and the basic legal issues involved * Recognize digital crimes |
|  | **4 min** | **TRACKING VS IDENTITY THEFT**  ***Review* slide**  *Ask* :   * **What is tracking, and how is it different than identity theft?**   + **Tracking is** **legal,** identity theft is illegal   + Tracking is done for surveillance or profit, identity theft is done to facilitate illegal theft and other illegal activities   + **Tracking does not try to impersonate you,** instead gathers information about your behaviour online to build a profile about you * **Who is likely to track you? What are their motivations?**   + Government agencies -> security, data collection   + Companies -> sell your data to advertisers, or make targeted ads themselves   + Browsers or search engines, to optimize your experience, such as remembering passwords, and providing local recommendations | * Listen to trainer * Discuss * Ask questions | * Recognize and critique government and corporate digital surveillance, the motivations and the basic legal issues involved * Recognize digital crimes |
|  | **4 min** | **MOST COMMON VULNERABLE PASSWORDS**  *Ask***:**   * **What do you notice about many of these passwords**?   *Answers:*   * **Sequential** or shape-based (keys next to each other) * Default passwords that come with a new system * **Simple words** that are in the dictionary * Simple, **common phrases**   *Explain* how computer programs can use **“brute force” attacks**, which involve guessing a lot of passwords really quickly.  *Ask:*   * **What kinds of passwords are these attacks likely to guess?**   + Anything is a “password dictionary”, which includes all dictionary words and common passwords | * Listen to trainer * Discuss prompts * Ask questions | * Choose secure and memorable passwords |
|  | **4 min** | **MAKING A STRONG PASSWORD**  ***Review slide***  *Emphasize* using passphrases  [Background reading: Creating Strong Passwords by Surveillance Self-Defense <https://ssd.eff.org/en/node/23/> ] | * Listen to instructor | * Choose secure and memorable passwords |
|  | **3 min** | **2 STEP VERIFICATION**  ***Explain* 2-step verification** and how it is one way to **increase security** to some of your accounts.   * Creates a two-step process when logging in. i.e. enter a password first, then a secondary piece of information, such as a **code sent to you by text**. * **Offered mainly by email and social media accounts** * Even if someone has your password, they can’t use it to get into your account unless they also have access to your phone, which hopefully you have locked with a different password. | * Listen to trainer * Ask questions | * Choose secure and memorable passwords |
|  | **5 min** | **PASSWORD MANAGERS**  ***Review* slide and explain what a password manager is**   * + **Writing down the passwords in a secure place** (journal in a locked drawer at home) **is also a possibility** if you don’t want them online. But this makes it hard when you are using multiple devices or are not at home etc.   ***Refer* to handout**: popular password managers are listed  *Direct* attention to the **“Assessing The Security of Your Accounts” chart** in the handout and e*xplain* to learners that they can **tackle this when they get home** as a tool to help them assess the security of their passwords to different accounts. | * Listen to instructor * Ask questions | Identify, select and manage support services for account management as needed (e.g. password managers) |
| **lll.png** | **8 min** | **PHISHING**  *Play* video [5:01]  *Ask:*   * Any **questions or comments** about the video?   *Review* content from video.  *Ask:*   * **What are some clues that an email might not be legitimate?**   + Suspicious email address   + Unknown source   + Spelling errors   + Link within email   + Does not include any information about you in it * **What’s the best way to avoid falling for a phishing email?**   + Do not click links in emails from sources you are unsure of   + Do not reply to spam emails   + If it looks like a legitimate organization, find that organizations contact information from another source and contact them directly | * Watch video * Ask questions | * Identify sensitive digital information for security purposes in personal and professional contexts * Recognize digital crimes * Examine and assess the consequences of sharing data online |
|  | **3 min** | **MALWARE AND ANTIVIRUS PROGRAMS**  ***Review* slide and explain malware and antivirus software**   * Malware is any **software designed to damage your computer** or gain unauthorized access to your files (can be used to steal data) * **Antivirus programs and firewalls** **protect your computer** from hackers and viruses online by scanning incoming network traffic to make sure it’s safe. Antivirus software can also scan and remove suspicious files that are already on your machine (see handout) * **Avoid click suspicious links**, downloading anything if you don’t trust the source. | * Listen * Ask questions | * Recognize digital crimes |
|  | **5**  **min** | **DID WE LEARN HOW TO…?**  ***Review* slide** and spend time answering any questions.  *Ask:*   * Do you have any other **questions and/or comments?**   ***Refer* learners to resources on the handout** and remind them to **find further resources on VPL research guides.** | * Listen * Ask questions |  |
| H:\PLG\Privacy\privacyslideshow\Slide20.PNG | **5 min** | **EVALUATION FORMS**  *Ask* them to take some time to **fill out the evaluation form.** If possible, have them **fill out the form online.** If not, provide them with the **paper forms**.   * We would like your feedback! Please take some time to fill out an evaluation form to let us know what you enjoyed and what could be improved. * There is a **bookmark link** to the form on all computers. * You can also access the link by going to <http://www.vpl.ca/trainingfeedback> |  |  |

## Closing

* Thank learners for coming
* Give out certificates to learners who came to all three classes