

Facilitator Guide



Contents

Background.....	2
Digital Privacy Programs.....	3
Digital Privacy 101.....	3
Digital Privacy 201.....	3
Conducting the Programs.....	3
Digital Privacy 101: Discussion and Activities.....	3
Digital Privacy 201: Discussion and Quiz.....	4
Role of the Facilitator.....	4
During the Workshop.....	5
Scripts, PowerPoint, and Resources.....	5
E*vents listing.....	5
Further knowledge.....	7
Privacy 101 Resources.....	7
Privacy 201 Resources.....	9

Background

TPL’s Digital Privacy initiatives are grounded in working to offer programs and services to help Torontonians have the digital literacy skills they need to succeed in the digital world.

Digital Literacy skills cover many areas, but it is important to teach our communities the importance of privacy when using your own digital devices or using a public computer. Privacy can easily be compromised but it is also possible to maintain your privacy by developing good habits.

Our dependency on computers and mobile devices is growing, daily we access all sorts of services, information, social media and so much more. So what happens when we use our devices, how secure are they, is there anything I should be doing, what happens to our data. As library staff we are faced with these questions and much more. Toronto Public Library recognized a need to educate our communities on how to protect their privacy online by launching digital privacy programs in 2016. In 2023, the series was audited and revised. The series contains two beginner-level programs: Digital Privacy 101 and Digital Privacy 201. The lecture-based program also includes a few interactive elements, such as discussion questions and a short quiz (applicable to Privacy 201) to test your knowledge.

The Digital Privacy series covers many areas: how to secure our accounts and devices; how to develop a strong password; learn about online threats; understand web browsers and search engines; how to reduce privacy risks; and how to stay safe using social media.

Digital Privacy Programs

Below are the learning objectives for each part of the series.

Digital Privacy 101

Learning objectives are the following:

1. Learn how to maintain your online privacy through good habits and through securing your accounts and devices.
2. Develop a strong password and review the best methods for storing your passwords.
3. Learn about various online threats: malware, phishing, hacking, etc.
4. Gain an understanding of the limitations of these tools and habits.

Digital Privacy 201

Learning objectives are the following:

1. Developing an understanding of web browsers and search engines
2. How to secure your web browser
3. Reduce privacy risks through the use of web browser plug-ins/extensions
4. Understand the privacy considerations of using social media

Conducting the Programs

Before conducting a program, it is recommended to read through the scripts and familiarize yourself with the content.

There are a few hands-on activities. Please review the activities, test them out with a colleague beforehand and if needed make a few tweaks, this brings in your own style.

Digital Privacy 101: Discussion and Activities

- Discussion (Slide 3) Opener questions, investigating knowledge
- Activity (Slide 6) Check for Software Updates
- Activity (slide 14) Creating a strong password

- Discussion (Slide 15) Using different passwords and storing/remembering passwords
- Discussion (Slide 26) Experiencing Malware and pointing to resources specific to online fraud.

Load necessary websites.

- Diceware – method for generating passphrases: (<https://www.eff.org/dice>)
- Word List for developing a passphrase: eff.org/files/2016/07/18/eff_large_wordlist.txt
- Roll a Dice <https://rolladie.net/>
- Privacy Breach Management (Government of Canada)
- <https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/breach-management.html>
- Canada's Anti Fraud Centre: <https://www.antifraudcentre-centreantifraude.ca/index-eng.htm>
- Government of Canada: Get Cyber Safe: <https://www.getcybersafe.gc.ca/en>

Digital Privacy 201: Discussion and Quiz

- Discussion (Slide 9) Browsers and search engines
- Activity (Slide 11) Searching permissions on a computer
- Quiz (Slide 20-24) Answers are in the notes field in the PowerPoint.

When setting up the program, it is advised to set up registration. Set the maximum number of participants to what you are comfortable with and keep in mind how many computers/laptops you have available and in good working order.

If you are using laptops, test to make sure each one is in full working order.

Please ensure Wi-Fi is working in the room you are offering the program as participants may be bringing in their own devices.

Print out the resource handout for participants.

Role of the Facilitator

Participants taking the program are not sure of the content, this may be the first time they are learning the concepts you are presenting.

If you are presented with a question and not sure of the answer, tell them you are not sure—be honest. Then proceed to figure it out together. This message should be included in your introduction.

The series is a start to their lifelong digital literacy journey—be patient.

During the Workshop

Introduce yourself

Set the ground rules and housekeeping items

Get to know the participants at the beginning, ask them what they want to get out of the session.

Ask what devices they have brought to the session.

Provide an overview of what they will be accessing during the workshop

The programs have several discussion questions and activities. Take breaks after each section, the slides indicate when the section ends. This is an opportunity to ask if there are any questions.

Scripts, PowerPoint, and Resources

Below is where you can find where you can retrieve scripts, PowerPoints and resources.

It is advised to retrieve PowerPoints, resources, and the facilitator guide each time you plan to run this program. Information may change throughout the year and revisions are made and updated within SharePoint.

Digital Privacy 101

[ShareTPL/UserEducation/scripts and handouts/Class Handouts Digital Privacy 101](#)

Digital Privacy 201

[ShareTPL/UserEducation/scripts and handouts/Class Handouts Digital Privacy 201](#)

E*vents listing

Below is what you would insert in E*vents. Please copy and paste.

Program title: Digital Privacy 101

Audience: Adults and Older Adults

Duration: 90 min

Description:

Are you interested to learn how to maintain your online privacy and how to secure your online accounts and devices? If so, this is the class for you. Come and join us in this introductory session that is filled with hands-on activities and discussion.

In this program, you will:

1. Learn how to maintain your online privacy through good habits and the security of your accounts and devices.
2. Develop a strong password, and review the best methods for storing your passwords.
3. Learn about various online threats: malware, phishing, hacking, etc.
4. Gain an understanding of the limitations of these tools and habits.

Registration is required.

Pre-Requisites: Some computer experience *required*; the ability to navigate app menus, browsers, and desktop computing features is desirable.

If you identify as a person with a disability or as a person who is Deaf, and require an accessibility accommodation to participate in this program, please contact Accessibility Services by email, accessibleservices@tpl.ca, or voicemail, 416-393-7099, to make a request. Please contact us at least three weeks in advance.

Program title: Digital Privacy 201

Audience: Adults and Older Adults

Duration: 60 min

Description:

Are you interested how to navigate the internet on your personal devices with improved privacy and understand the importance of how to stay safe using social media? If so, this is the class for you.

In this program, you will:

1. How to use public computing environments with improved privacy
2. Navigate the Internet on your personal devices with improved privacy
3. Reduce privacy risks through the use of web browser plug-ins/extensions
4. Understand the privacy considerations of using social media

Registration is required.

Pre-Requisites: Some computer experience is *required*; the ability to navigate app menus, browsers, and desktop computing features is desirable.

If you identify as a person with a disability or as a person who is Deaf, and require an accessibility accommodation to participate in this program, please contact

Accessibility Services by email, accessibleservices@tpl.ca, or voicemail, 416-393-7099, to make a request. Please contact us at least three weeks in advance.

System-Wide Promotion

Digital Privacy is recognized by TPL through several yearly key events. Privacy Programs occurring during these times are promoted at a system-wide level via e-newsletter, social media channels and TPL's homepage. Listed below are key event dates that we recommend branch staff include in their planning calendar:

- Data Privacy Week - the last week in January
- Cybersecurity Month –September
- Privacy Awareness Week – First week of May
- Digital Inclusion Week - First week in October

Information leading up to the week will be shared via Public Service Announcements and Yammer.

Further knowledge

Books (Available through TPL's catalogue)

- [The Fight for Privacy: Protecting Dignity, Identity and Love in the Digital Age](#) by Danielle Keats Citron. 2022 (available as an e-book)
- [Privacy is Power: Why and How You Should Take Back Control of Your Data.](#) 2020 (available as an e-book)
- [Digital for Good: Raising Kids to Thrive in an Online World](#) by Richard Culatta . 2019 (available as an e-book)
- [Internet for the People: The Fight for Our Digital Future](#) by Ben Tarnoff. 2022. (available as an e-book)

Privacy 101 Resources

- [Slouching Toward 'Accept All Cookies' \(The Atlantic\)](#)
- [What Digital Privacy Is Worth \(The Atlantic\)](#)
- [The Battle for Digital Privacy Is Reshaping the Internet \(The New York Times\)](#)
- [Should We Chat? Privacy in the WeChat Ecosystem \(The Citizen Lab\)](#)
- [California Takes Some Big Steps for Digital Rights | Electronic Frontier Foundation \(eff.org\)](#)

- Citizen Lab's Security Planner (online tutorial tool): <https://securityplanner.org>
- Electronic Frontier Foundation Surveillance Self-Defence Security Starter pack: <https://ssd.eff.org/en/playlist/want-security-starter-pack>
- Electronic Frontier Foundation Basic tips for digital security: <https://ssd.eff.org/en/module/seven-steps-digital-security>
- Security in a Box: Digital Security Tools and Tactics: <https://securityinabox.org/en/>
- Schneier on Security: <https://www.schneier.com/>
- Umbrella App on Google Play: The all-in-one app for digital and physical security : <https://play.google.com/store/apps/details?id=org.secfirst.umbrella&hl=en>

Passwords

- Have I Been Pwned? – online data breach tracking website (<https://haveibeenpwned.com/>)
- John the Ripper – open source password cracker software (<https://www.openwall.com/john/>)
- Zxcvbn library - password strength checker (<https://www.bennish.net/password-strength-checker/>)
- Diceware – method for generating random memorable passphrases (<https://www.eff.org/dice>)
- Bitwarden – an online password manager (<https://www.bitwarden.com>)
- Mooltipass – hardware password manager (<https://www.themooltipass.com/>)
- Yubikey – hardware 2FA token (<https://www.yubico.com/products/>)

Privacy Breach resources

- Privacy Breach Management (Government of Canada)
- <https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/breach-management.html>
- Canada's Anti Fraud Centre: <https://www.antifraudcentre-centreantifraude.ca/index-eng.htm>
- Government of Canada: Get Cyber Safe: <https://www.getcybersafe.gc.ca/en>

Privacy 201 Resources

Browsers

- Online Marketing: <https://www.bdc.ca/en/articles-tools/entrepreneur-toolkit/templates-business-guides/glossary/online-marketing>
- Best secure browsers to protect your privacy online: <https://www.zdnet.com/article/best-browser-for-privacy/>
- Google Privacy Sandbox : <https://privacysandbox.com/>
- Firefox Blocks Fingerprinting : <https://www.mozilla.org/en-CA/firefox/features/block-fingerprinting/>
- TOR New identity: [MANAGING IDENTITIES | Tor Project | Tor Browser Manual](#)
- What is a VPN? : <https://ca.norton.com/blog/privacy/what-is-a-vpn?lsModal=1>

Privacy and Ad Blocker browser extensions

- What are browser extensions, and are they safe?: <https://brave.com/learn/what-are-web-browser-extensions/>
- Why do I have to click to activate plugins? : <https://support.mozilla.org/en-US/kb/why-do-i-have-click-activate-plugins>
- EFF Privacy Badger : <https://privacybadger.org/>
- uBlock Origin - Free, open-source ad content blocker: <https://ublockorigin.com/>
- RIP uBlock Origin? Google Proceeds With Plan to Shake Up Chrome Extensions (article): <https://www.pcmag.com/news/rip-ublock-origin-google-proceeds-with-plan-to-shake-up-chrome-extensions>
- AdBlock (Android mobile app): <https://getadblock.com/en/>
- TrustGo (Android mobile app): <https://www.trustgo.com/>

Backing up devices

- Backing up your Windows PC: <https://support.microsoft.com/en-us/windows/back-up-your-windows-pc-87a81f8a-78fa-456e-b521-ac0560e32338>
- Backing up a MacOS: [Back up your Mac with Time Machine - Apple Support \(CA\)](#)
- How to backup your Android phone: [How to back up your Android phone - Android Authority](#)
- How to back up your iPhone: [Back up iPhone - Apple Support \(CA\)](#)
- Cloud Security Issues & Challenges (Article): <https://www.kaspersky.com/resource-center/preemptive-safety/cloud-security-issues-challenges>

Social Media

- Get Cyber Safe (Government of Canada): <https://www.getcybersafe.gc.ca/en/secure-your-accounts/social-media>