Online Safety

Workshop 3

October 2026



AlphaPlus





Links

https://docs.google.com/document/d/1ToXVFvvHUlWtygQt5jJp9UD8WCR1aJZES8jNAGHh6To/edit?usp=sharing

AlphaPlus

Learn together

Privacy and personal data

Today we are going to look at privacy tools and practices that can keep us safer and protect our data.

We are going to look at

- what online privacy means;
- our rights and protections;
- how we can protect our data and privacy.

1. Part 1: Learning about online privacy
2. Part 2: Implementing online privacy practices
3. Part 3: Digging deeper







Part 1: Learning about online privacy

Slides 4 to 24 are lessons to guide discussions about online privacy.

The ideas come from

Curriculum Resources

Mozilla (New)

- Safety First lesson

MediaSmarts (Workshops 1 and 2) **FR**

- DigitalSmarts Online Privacy Workshops Explore, Discover, and Navigate

DigitalLearn.org (Workshops 1 and 2)

- Being Safe Online Series: Internet Privacy
- Teacher Site

Teacher Resources

EFF - Electronic Frontier Foundation (New)

- Cover Your Tracks
- Test Your Browser



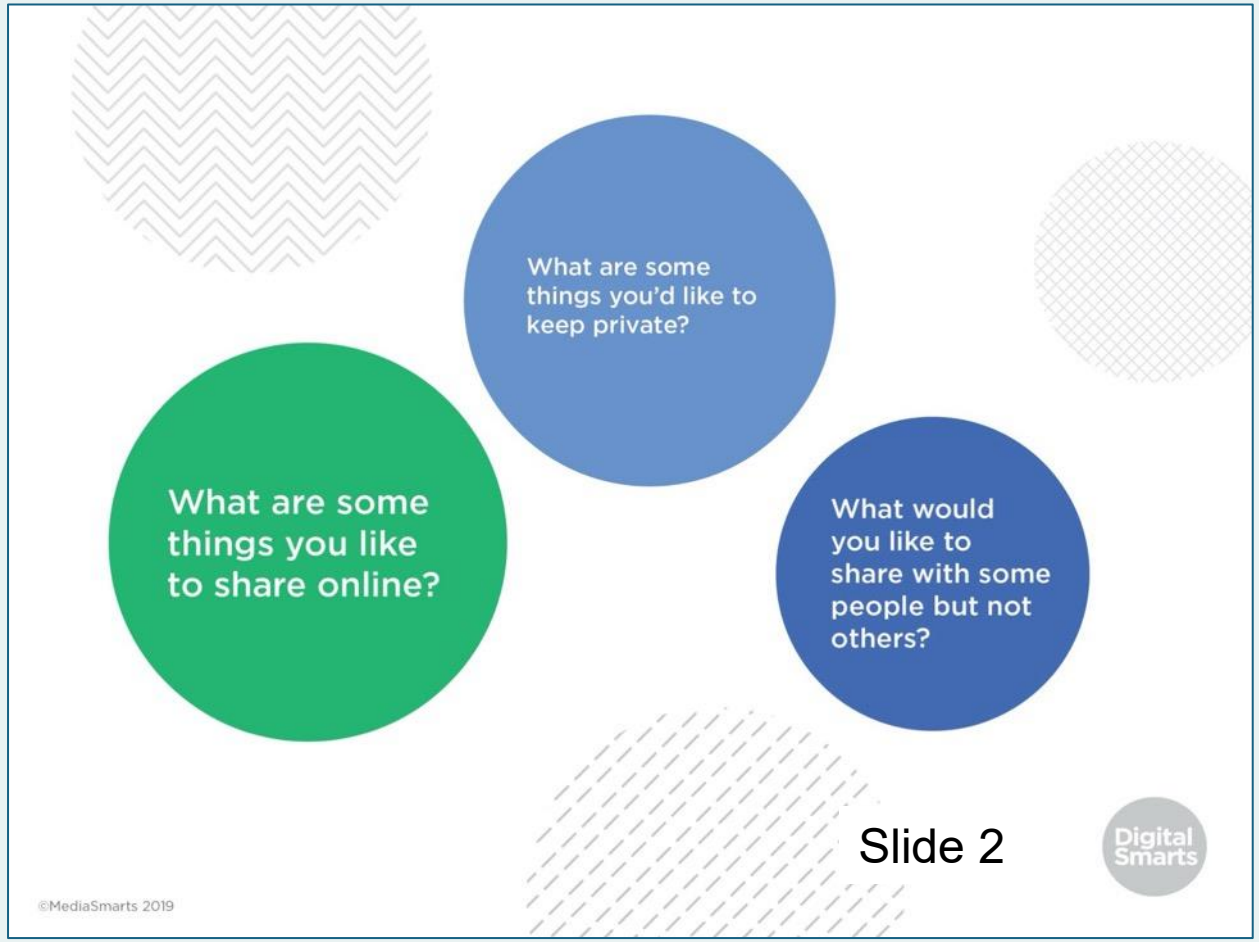
See more about these resources in the **Annotated Bibliographies**

Curriculum Resources

Teacher Resources

AlphaPlus

Early Bird Reflection



As we are getting ready…

You don't have to share your answer. Just think about –

- What are some things you like to share on the internet?
- What are some things that you'd like to keep private?
- How do you think the internet could help you do those things?

From MediaSmarts DigitalSmarts ***Explore*** *Online Privacy* Workshop.

AlphaPlus

Welcome

It is lovely to see you all.

To get us started, tell us

- When you hear the word “privacy,” what do you think about?
- How does the concept of privacy apply to your everyday life?

Padlet

https://padlet.com/traceyehm/privacy3_warmup



Questions from Mozilla’s Safety First lesson.

The links in this lesson are mostly broken but the questions and activities are interesting.

Online Privacy



How do the notions of privacy we shared work in the context of what we do on the web?

Does privacy apply equally to your offline life and your time on the web?

Why / why not?

What are you already doing to protect your privacy?

- Checklist (Google Form)
- https://forms.gle/fytp8ZyP65NXWWU16

Questions from Mozilla's Safety First lesson.

Make your own copy: https://docs.google.com/forms/d/1yGsc0rrWUa17Of7d0CgjJfmzhrYSoaUW9CFdkp3u3WY/copy

AlphaPlus

My day so far



My Day (So Far)
Use this worksheet to make a list of what your activities so far today. For each item on your, answer the following questions:

- What did I do?
- When did it happen?
- What device did I use?
- Did I visit any websites to accomplish the task?

My name:
Today's date:

My journal:

[Try the Activity in Google Slides]

https://docs.google.com/presentation/d/1u5hcrc565KqnwhP3eLz0P9h_dx-0z3XRCCLMadZNj70/edit?usp=sharing

[A clean copy – you can make your own copy]

https://docs.google.com/presentation/d/19DCDOfqHU7YmfBLEhn_ZQ5eTemQkNnbrEdY1ja1OTH0/edit?usp=sharing

Your day online



Don't worry if you do not know all the answers.

That is what we will talk about next.

- How many of your actions today included technology?
- Did the number of tasks that relied on technology surprise you?
- How many of your actions today required the use of a website?
- Who might notice how often you are using technology to do day-to-day tasks?
- What could they find out about your online habits?
- What could they find out about where you are in the real world?
- **What information would you like to protect?**

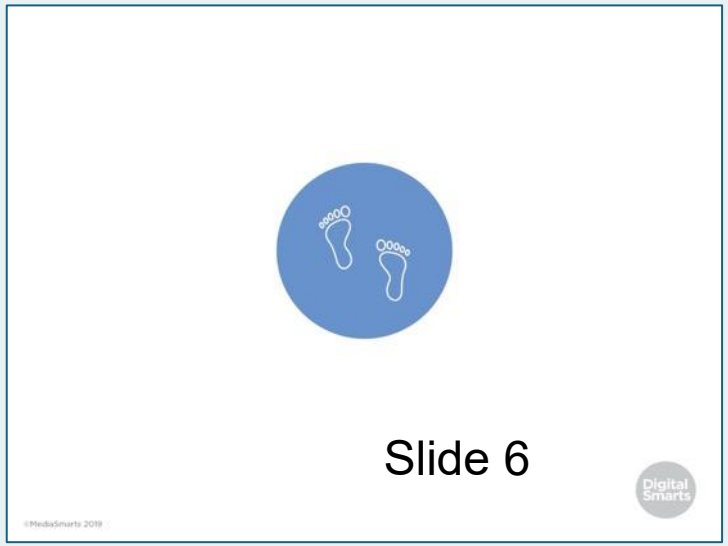
Footprints and shadows



The information we leave behind as we travel through the web is what is known as a “digital footprint”.

Your digital footprint includes websites you visit, emails you send, and information you provide to online services.

Everything is connected



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

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

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

From MediaSmarts DigitalSmarts
Explore *Online Privacy* Workshop.

Our information

While browsing the Internet, we are constantly sending and receiving information from various websites and individuals.

When we send and receive information, we can take control of who is able to see that information, and how much information they can see. Internet privacy refers to the level of personal, private information we share.

Information from DigitalLearn.org

Being Safe Online Series: Internet Privacy

Teacher Site

Online tasks

Here are four common tasks on the Internet that involve sharing information:

- Searching the web
- Visiting a website
- Online shopping
- Social media

Some information should be completely private, like credit card numbers and passwords. Other times, we may want to share something with others, but limit who can see it.

Online tasks and our information

Searching	Visiting a site	Shopping	Social media
When searching the web, your searches are often saved on the computer you're using. The search engine company can also see information about what you're searching for. Web browsers have settings you can apply to control the information that is tracked and saved.	Any time you visit a website, the owner of the website can see general information about the type of computer you are using and what you are doing on the site.	Online shopping requires sending information like your passwords and credit card numbers to a website. You'll want to make sure the website is trustworthy and this information will be kept private.	Social media sites are all about sharing. You can share things publicly, with groups of people, or with individuals. Social media companies have access to some information about what you share.

Searching

You want to buy a pair of shoes online. What privacy issues should you think about when **searching the web** and **visiting a website**?

Searching the web

When we use a search engine to search online, information is tracked on our keywords. Web browsers include **privacy settings** that allow us to control what is stored and tracked.

To be as private as possible, open a private browser window (slide). This will keep search engines from tracking you as you search and will keep the browser from saving your search history.

Visiting a website

Any time you visit a website, information is collected, including your **geographic location**, the **links you click on**, and other **information about your web browser, computer, or other device you're using**.

This information generally doesn't identify you as an individual but gives the website owner helpful information about who comes to the website and technologies their visitors use.

Some websites collect more specialized information. They may scan for keywords you use and use those words to show advertisements.

Making an account

If you create an account on a website, the site owner will also have access to information like your

- name,
- email address,
- or even your physical address and phone number.

They could use this information to send you marketing emails or letters.

Cover Your Tracks



When you visit a website, your browser makes a "request" for that site.

Each request contains several pieces of information about your browser and about you, from your time zone to your browser settings to what versions of software you have installed.

Some of this information is simply to help you view the page.

Some of the information is extracted by third-party ad networks, which have tracking mechanisms embedded across the internet to gather information about you.

EFF - Electronic Frontier Foundation

- Cover Your Tracks
- Test Your Browser

Third-Party Advertising Networks



The first party is the website you are visiting.

The second party is you.

The third party is an advertiser.

A fourth party is an advertising server or network.

The website owners (first party) sell access to your attention (second party) to advertisers (third parties) through an ad server (fourth party).

Ad servers such as Google (AdWords and AdSense) bring together consumers, websites and advertisers. The ad server seeks website operators that want to place advertising on their sites. The operators place code or script that allows the server's network to appear in the ad space. The server also recruits advertisers that want to place ads on the available network of sites. The advertiser buys a certain amount of ad buys or spaces and takes a cut of the revenue before passing it on to the website operator.

Cookies and Fingerprinting



The individual bits of data that third-party trackers collect may not seem that dangerous but when put together, they can reveal a detailed profile of your online activity, from political affiliation to education level to income bracket.

Ad networks use two methods to keep the data they collect linked to specific users:

- cookie tracking
- browser fingerprinting

Cookie Tracking



🍪 Cookies are small chunks of information that websites store in your browser.

😀 Their main use is to remember helpful things like your account login info, or what items were in your online shopping cart—in other words, they save your place.

😈 But they can also be used to link all your visits, searches, and other activities on a site together. This use of cookies is a privacy violation, and browsers generally allow you to block, limit, or delete cookies.

Fingerprinting



👇 A digital fingerprint is essentially a list of characteristics that are unique to a single user, their browser, and their particular hardware setup.

😀 This includes information the browser needs to send to access websites, like the location of the website the user is requesting.

😈 But it also includes a host of seemingly insignificant data (like screen resolution and installed fonts*) gathered by tracking scripts. Tracking sites can stitch all the small pieces together to form a unique picture, or "fingerprint," of your device.

*Used to help the browser render the page properly.

More information: [Your Browser Is Leaking Information About You. Here's How to Stop It] from PCMag

AlphaPlus

Cookies and Fingerprinting compared



Cookies are temporary and work until the user deletes them

Cookies are similar to the small tracking devices scientists use to follow animal migration patterns, or a GPS transmitter attached to a car. As long as they're attached to the target animal or vehicle, they are accurate and effective—but they lose all value if they're knocked off or discarded. (You can clear your cookies.)

Fingerprinting is more permanent and the markers cannot be changed or deleted

Fingerprinting identifiers include hardware specifications and browser settings. This is similar to tracking a bird by its song or feather markings, or a car by its license plate, make, model, and color.

Try this



1. Pick a website that you want to know more about.
2. Go to Blacklight (https://themarkup.org/blacklight)

   Enter the address of any website, and Blacklight will scan it and reveal the specific user-tracking technologies on the site—and who's getting your data.
3. Enter the website address to see the trackers they are using.
   - What did you see in Blacklight that surprised you about online tracking?
   - Are there important, "good" reasons to track people online that are worth losing some privacy over?



Part 2: Online privacy practices

Slides 26 to 50 are lessons and resources to support the implementation of privacy practices.



Curriculum Resource

MediaSmarts FR

- DigitalSmarts Online Privacy Workshops
  Explore, Discover, and Navigate (Workshop 1 and 2)

Teacher Resources

Office of the Privacy Commissioner (New) FR

Government of Canada

- Get Cyber Safe (Workshop 1 and 2) FR

EFF - Electronic Frontier Foundation (New)

- Opt Out October: Daily Tips to Protect Your Privacy and Security

See more about these resources in the **Annotated Bibliographies**

Curriculum Resources

Teacher Resources

AlphaPlus

What can we do?



Know your rights

Develop privacy practices

Learn about privacy settings

- Secure your devices - tips
- Secure your phone
- Browser privacy settings
- Secure your connections
- Private browsing and incognito mode
- Browser extensions that protect your privacy
- Choose browsers and search engines that protect privacy

Know your rights



From buying groceries at the store to shopping for clothes online to paying for a service like a renovation, modern commerce often involves personal information.

But sharing your personal information with businesses doesn't mean giving up control over it.

Office of the Privacy Commissioner

- A PowerPoint Presentation
- Speaking Notes (PDF)

AlphaPlus

PIPEDA - The Personal Information Protection and Electronic Documents Act



PIPEDA sets the ground rules for handling personal information in the course of commercial activities. It applies equally to small and big businesses, whether they operate out of an actual building or only online.

PIPEDA requires businesses to collect, use or disclose your information by fair and lawful means, with your consent, and only for purposes that are stated and reasonable. Basically, they can only collect personal information that's essential to their product or service. If they want more, you can ask why, and you're entitled to decline to provide it, while still being able to complete your transaction.

More information

AlphaPlus

What is personal information?



The Personal Information Protection and Electronic Documents Act (PIPEDA) protects information that is identifiable to an individual.

What is personal information?

Think of the things that make you unique, like your fingerprints. In the same way, there is data specific to your life, like your credit card information and tax returns.

Office of the Privacy Commissioner

- A PowerPoint Presentation
- Speaking Notes (PDF

AlphaPlus

Personal information (1/2)



Personal information includes your:

- Name, race, ethnic origin, religion, marital status, educational level;
- Email address and messages, IP (Internet protocol) address
- Age, height, weight, medical records, blood type, DNA code, fingerprints, voiceprint (the characteristics of your voice);

Personal information (2/2)



Personal information includes your:

- Income, purchases, spending habits, banking information, credit/debit card data, loan or credit reports, tax returns;
- Social Insurance Number (SIN) or other identification numbers.
- Personal information can also include the words you type, the websites you visit and the photos you post.

AlphaPlus

Making a report



From time to time, you might be concerned about how an organization is handling your personal information.

A good place to start is to bring up your concerns directly with the business. Often, they can resolve the issue quickly.

Tips for raising your privacy concern with a business

If you're not satisfied with how the organization responds, you have every right to issue a complaint through the OPC. You don't need a lawyer or consultant to do it. Online, the Office of the Privacy Commissioner has a guide to the complaint process. It also has an information phone line staffed with officers to help answer specific questions you may have about privacy-related issues.

Report a concern

Privacy practice: Think twice (1/3)



Online and in person, we're constantly being asked for our personal information.

Don't just give it up.

Think about why the organization needs it, who will use it, and how. If you're not sure, ask.

If you're not comfortable with the answers you receive, let the organization know, and don't give out your personal information. That might mean not using the product or service the organization provides.

10 tips for protecting personal information

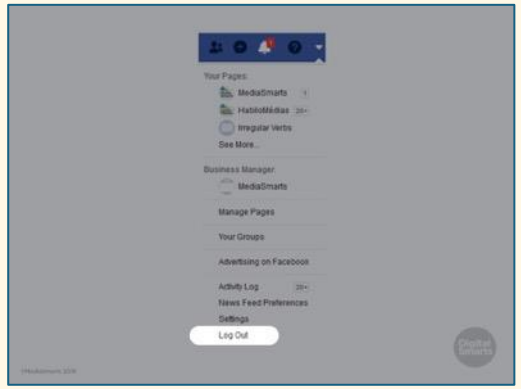
Privacy practice: 3 tips (2/3)

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

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

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



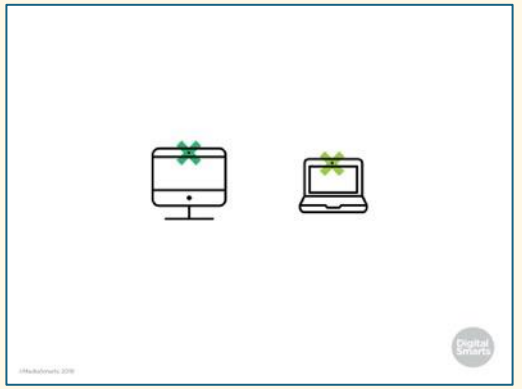


Slides 8 and 9

From MediaSmarts
DigitalSmarts ***Explore***
Online Privacy Workshop.

Privacy practices (3/3)

3. You can also **cover the cameras** on laptops and other devices when you're not using them so that you can't be seen by them when you don't want to be. You can do this with a sticky note or something similar that's easy to take off when you want to use the camera.



Slide 8

From MediaSmarts DigitalSmarts ***Explore*** *Online Privacy* Workshop.

Privacy settings



Privacy settings aren’t a silver bullet, but they can definitely give you more control over your information. It’s important to know that default settings can leave you exposed.

Settings help you indicate whether or not you give consent for the collection, use and disclosure of your personal information.

It’s important to choose privacy settings that you are comfortable with on social media accounts, online services, devices and browsers.

You have a right to say “no” to providing personal information that isn’t integral to the product or service. Look for options to turn off actions like accessing your microphone or tracking your location if those actions are not required to use the service.

Tips for using privacy settings

Securing your devices



Set device passwords that are difficult to guess. That way, if you leave your phone somewhere by mistake, it’s much more difficult for someone to access your personal information.

You can also install anti-virus and security software on your devices. Be sure to keep this software updated.

Be sure to delete all personal information from your old devices (like your phone, laptop or tablet) before discarding, recycling or selling them. It’s worth noting that even restoring electronics to factory settings doesn’t permanently delete the data. Check with the device manufacturer.

Securing your devices tips



Government of Canada:
Get Cyber Safe

Secure your devices

- Laptops and computers
- Phones and tablets
- Storage and backup
- System updates
- Gaming systems
- TVs and smart devices

Office of the Privacy Commissioner

Mobile devices

- Protecting your information on mobile devices
- Tips to protect your inbox, computer and mobile device
- Your privacy and mobile apps
- Wearable devices
- Gaming and personal information: playing with privacy

Securing your phone



EFF (Electronic Frontier Foundation)

The Electronic Frontier Foundation a nonprofit organization defending civil liberties in the digital world. EFF's mission is to ensure that technology supports freedom, justice, and innovation for all people of the world.

- How to: Get to Know Android Privacy and Security Settings
- How to: Get to Know iPhone Privacy and Security Settings

Opt Out October

- Tip 3: Disable Ad Tracking on iPhone and Android
- Tip 4: Declutter Your Apps
- Tip 7: Review Location Tracking Settings

Other privacy resources from EFF

Privacy

Surveillance Self-Defense

All Guides

(Security Scenarios are US based and laws may be different in Canada)

AlphaPlus

Browser privacy settings



The good news is that your internet browser has built-in tools to help protect your personal information.

Take some time to learn about the security and privacy settings in your browser and keep them up to date.

- Browse the web more securely

  from Security in-a-box

- Privacy settings in different browsers
  - Brave
  - Chrome
  - Edge
  - Firefox
  - Opera
  - Safari
- How to clear your browsing history

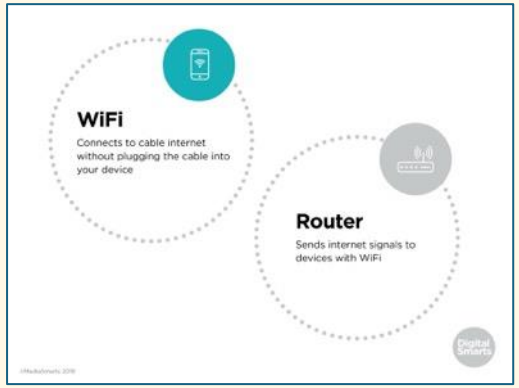
  from Computer Hope

Public and private networks

A lot of us use public WiFi in places like libraries or coffee shops. It's important to know that public WiFi is less secure than your home network.

Networks that don't make you enter a password are especially risky because anyone can connect to them. That means that people with the right programs can see what you're sending to the router, including your login and password and things like your credit card information.

It's more secure if you have to enter a password to connect to the network, but you're still sharing it with anyone else who might be connected.



Slide 8

From MediaSmarts [DigitalSmarts](#) ***Navigate*** *Online Privacy* Workshop.

Securing your connections



When surfing on public WiFi, avoid sensitive transactions such as online banking as the connection is not secure and others may be able to capture the data you are sending.

You should also disable WiFi and Bluetooth when you are not using it – when you leave your device open by default, you leave your data vulnerable to access by others without your knowledge or consent whenever you pass through cafés and other places offering open, public wireless networks.

Remember: While not foolproof, look for the lock icon, HTTPS protocol or green highlighting in the address bar. These are all signs the site is likely secure.

Government of Canada: Get Cyber Safe

Secure your connections

- Private networks
- Public WiFi
- Bluetooth

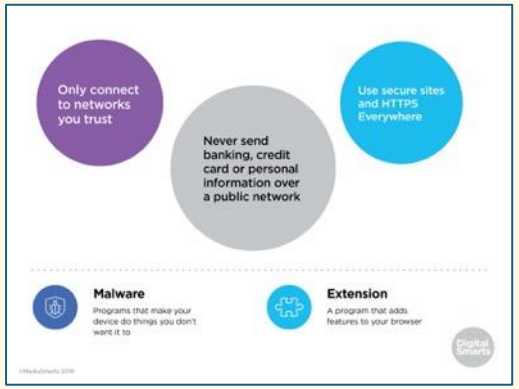
AlphaPlus

Public WiFi tips

There are 3 things you can do to make using public WiFi safer.

1. First, make sure that you're using a network you trust. You can give your network any name you want, so people sometimes set up fake ones called things like "Public Library" or "Starbucks Wifi" to spy on people or install malware on their computers. Double-check to make sure you're connecting with the right network.
2. Second, never do anything like online shopping or checking your bank account on public networks. Even on a secure network there's a chance that somebody might be able to see what you're sending.
3. Finally, stick to secure sites as much as possible. Those are the ones with a padlock in the address bar and a web address that starts with https, instead of just http.

The slide notes also say: You also should install the HTTPS Everywhere extension but it has been discontinued. Major browsers now offer native support for an HTTPS only mode. Learn how to turn it on.



Slide 9

From MediaSmarts DigitalSmarts ***Navigate*** *Online Privacy* Workshop.

Private browsing 1/3

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

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

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



Slide 11

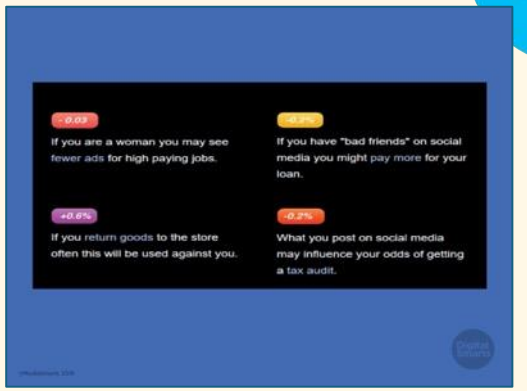
From MediaSmarts
DigitalSmarts *Explore Online Privacy* Workshop.

Private browsing 2/3

2. That matters because websites and advertisers use what they know to make a profile of you.

   They use that profile to decide what advertisements to show you, but it may also be used to decide everything from how much you pay for things to whether or not you can get insurance.

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





Slides 12 and 15

From MediaSmarts
DigitalSmarts *Explore Online Privacy* Workshop.

Private browsing tips 3/3

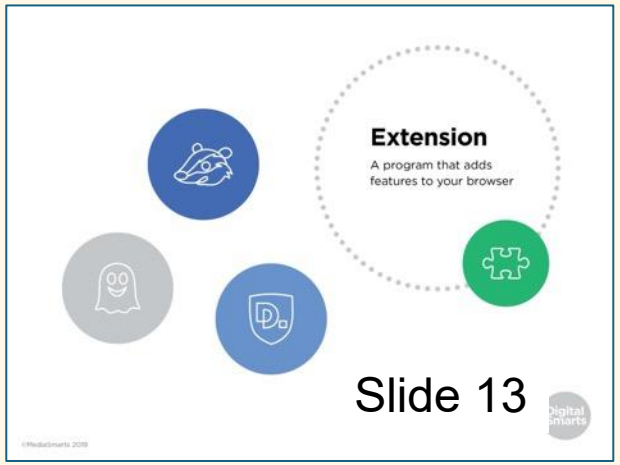


Private browsing (Firefox), InPrivate browsing (Edge), incognito mode (Chrome) or a private window, is an Internet browser setting that prevents browsing history from being stored. Normally, when you visit any web page, any text, pictures, and cookies required by the page are stored locally on your computer. Additionally, any searches or forms that are filled out may be stored in autocomplete fields. Incognito mode forgets this data when you close the browser window or doesn't store it at all.

More from Computer Hope:

- More about incognito mode
- How to set a browser to Incognito or private mode
- How to default launch a browser in private or incognito mode

Browser extensions



Extensions are little programs that work with your browser.

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

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

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

From MediaSmarts [DigitalSmarts](#) *Explore Online Privacy* Workshop.

AlphaPlus

Recommended browser extensions



- Privacy Badger from EFF is a free and open source browser extension that stops advertisers and other third-party trackers from secretly tracking where you go and what pages you look at on the web.

  About Privacy Badger from Wikipedia

- Ghostery is a free and open source browser extension and mobile browser application that prevents the collection of a user's browsing habits via cookies and more sophisticated forms of tracking such as canvas fingerprinting.

  About Ghostery from Wikipedia

- Disconnect is a partly open source browser extension and mobile app designed to stop non-consensual third party trackers and providing private web search and private browsing.

  About Disconnect from Wikipedia

Two more browser extensions



- AdBlock Plus is a browser extension for content-filtering and ad blocking.

  About AdBlock Plus from Wikipedia

- UBlock Origin is a free and open source browser extension for content filtering, including ad blocking.

  About Ublock Origin from Wikipedia

Choose browsers that protect privacy



Brave (Browser and Search Engine)

- Privacy Protections
  - Brave vs Firefox
  - Brave vs DuckDuckGo
  - Brave vs Everyone

Firefox (Browser)

- Browser Fingerprinting Protection
- Privacy Protections
  - Facebook Container Browser Extension
  - Multi-Account Containers Browser Extension

DuckDuckGo (Browser and Search Engine)

- Blog and Help Pages
- DuckDuckGo Search & Tracker Protection
  - DuckDuckGo Browser vs Chrome, Safari, Firefox and Brave
  - DuckDuckGo Browser vs Chrome, Safari, uBlockOrigin and AdBlock Plus

EFF Opt Out October

Tip 15: Switch to a Privacy-Protective Browser

AlphaPlus

Part 3: Digging deeper

Slides 52 to 57 offer some more advanced solutions such as

- Search engines and privacy
- Using encrypted email services
- Social media and account settings
- The difference between privacy and anonymity
- Using a Virtual Personal Network (VPN)

We won't cover this in the workshop but I put these slides here to help you in case learners ask questions about these things.

Most learners – most people – do not need these advanced privacy solutions if they are doing the other things mentioned in these slides.



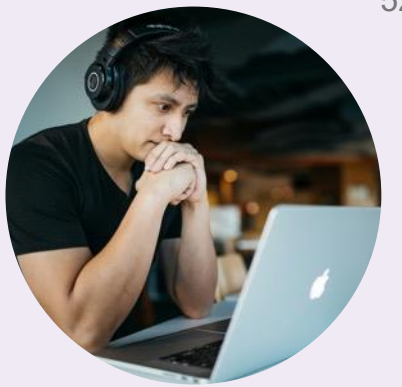
See more about these resources in the **Annotated Bibliographies**

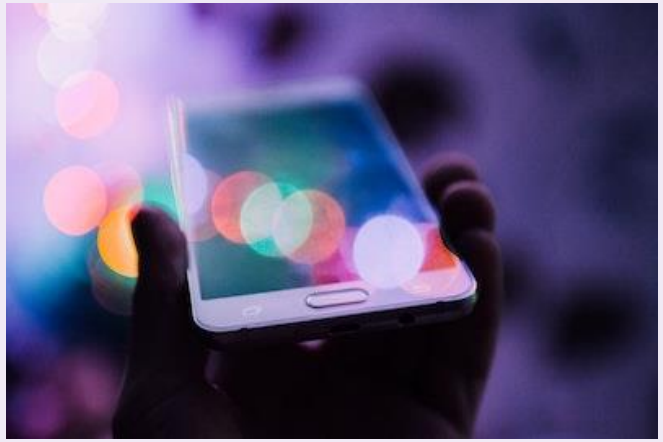
Curriculum Resources

Teacher Resources

AlphaPlus

Search engines and privacy



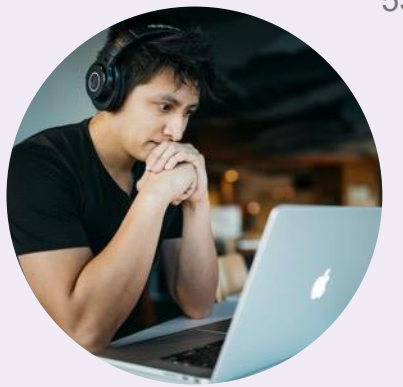


AlphaPlus workshop from January 2026

How can I turn everyday tech use into learning activities?

- Workshop 1 Slide Deck
  Basic searches, AI augmented searches and using chatbots to get answers to questions, using search skills on websites.

Email and Messaging Services



Email encryption protects the content of an email message from being read by entities other than the intended recipients.

Email is prone to the disclosure of information. Although many emails are encrypted during transmission, they are frequently stored in plaintext, potentially exposing them to unauthorized access by third parties, including email service providers. By default, popular email services such as Gmail and Outlook do not enable end-to-end encryption. Utilizing certain available tools, unauthorized individuals may access and read the email content.

Wikipedia

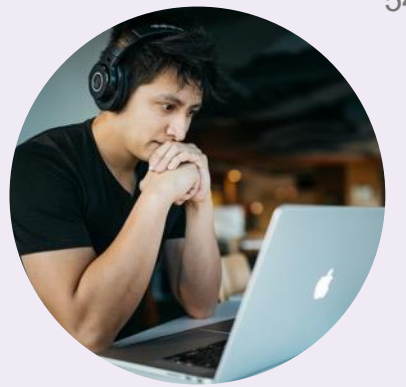
Some encrypted email services with free options

- Protonmail
- Tutanota
- Mailfence

Encrypted messaging

- Tip 14: Check Out Signal

Social media and account settings



From EFF Opt-Out October

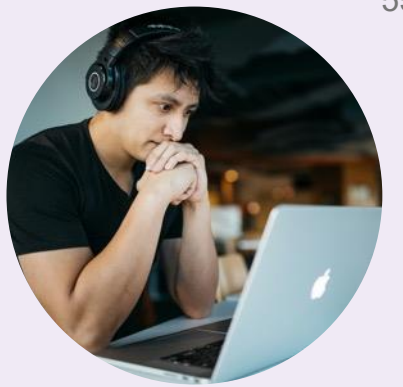
- **Tip 20: Tighten Account Privacy Settings**

- Tip 18: Minimize Risk While Using Digital Payment Apps
- Tip 19: Turn Off Ad Personalization to Limit How the Tech Giants Monetize Your Data
- Tip 21: Protect Your Data When Dating Online

- Tip 10: Find and Delete an Account You No Longer Use
- Tip 13: Remove Your Personal Addresses from Search Engines

Apple
Discord
Facebook
Google
Instagram
LinkedIn
Microsoft
Snapchat
TikTok
Twitch
Venmo
WhatsApp
X
YouTube

Staying anonymous online



Anonymity and privacy are not synonyms.

Privacy: controlling what data you release.

Anonymity: whether that data can be connected to you.

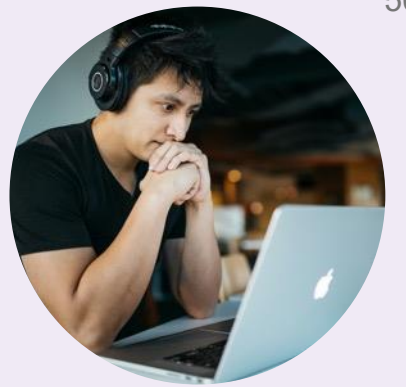
Think of **privacy** like being in your own home. People may know you live there, but when you draw the curtains, nobody can see what you're doing inside. Privacy means that you can limit what others know about you. Before you trust someone, you may tell them your name, but not your phone number or social security number.

Anonymity is like being a nameless face in a crowd. You're in public, so everybody can see what you're doing, but nobody knows you're the one doing it. When you're anonymous online, all your actions are visible -- they just can't be traced back to you.

From The Complete Beginner's Course to VPNs from Cloudwards (PDF).

This lesson provides plain language explanations of how a VPN works and how it can enhance your anonymity online and explains how anonymity is different than privacy. Very near the end it tells you how to use a VPN. It recommends certain VPNs and you may want to ignore that part.

What is a VPN?



VPN (short for Virtual Private Network) is a service that gives you an extra layer of protection online by encrypting your Internet connection across your entire device and hiding your location and IP address from the sites you visit.

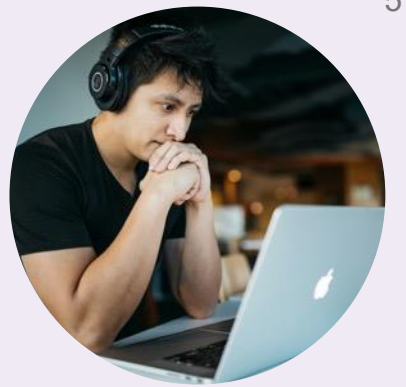
The Complete Beginner's Course to VPNs from Cloudwards (PDF).

This lesson provides plain language explanations of how a VPN works, how it can enhance your anonymity online and how anonymity is different than privacy. Very near the end it tells you how to use a VPN. It recommends certain VPNs and you may want to ignore that part.

What is a VPN and How Does it Work? video from Fluentize.
There is also a lesson from 2020 available for a fee but I did not want to give them my credit card info.

Introduction to VPNs from Network Lessons.com. These lessons are quite advanced.

Free VPNs



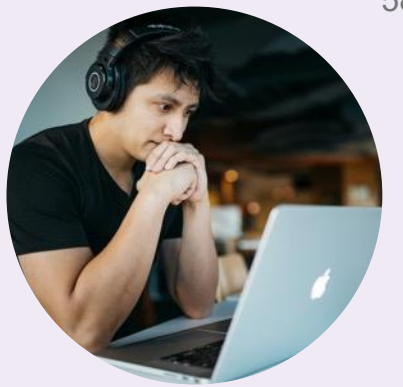
Firefox offers a built-in VPN feature that helps protect your browsing activity by routing it through a secure proxy server, masking your IP address. This feature is available for free to eligible users and is designed to enhance your privacy while using the Firefox browser.

Browser With Built-In VPN: Secure Browsing

A free VPN you can trust, now built into Firefox

Proton Free VPN

More about online anonymity



From the Mozilla Foundation – surveillance pricing

How to Disappear: Shopping Online: an article about surveillance pricing.

How to Skip Surveillance Pricing: A Guide: an article about how to protect yourself from surveillance pricing.

From Security in a Box – for people in danger from surveillance

Anonymize your connections and communications

This guide explains how to anonymize connections and communications to achieve a specific goal without leaving any traces. This strategy is particularly helpful in high-risk situations where your activities cannot be connected to your identity as this would compromise your freedom and wellbeing.



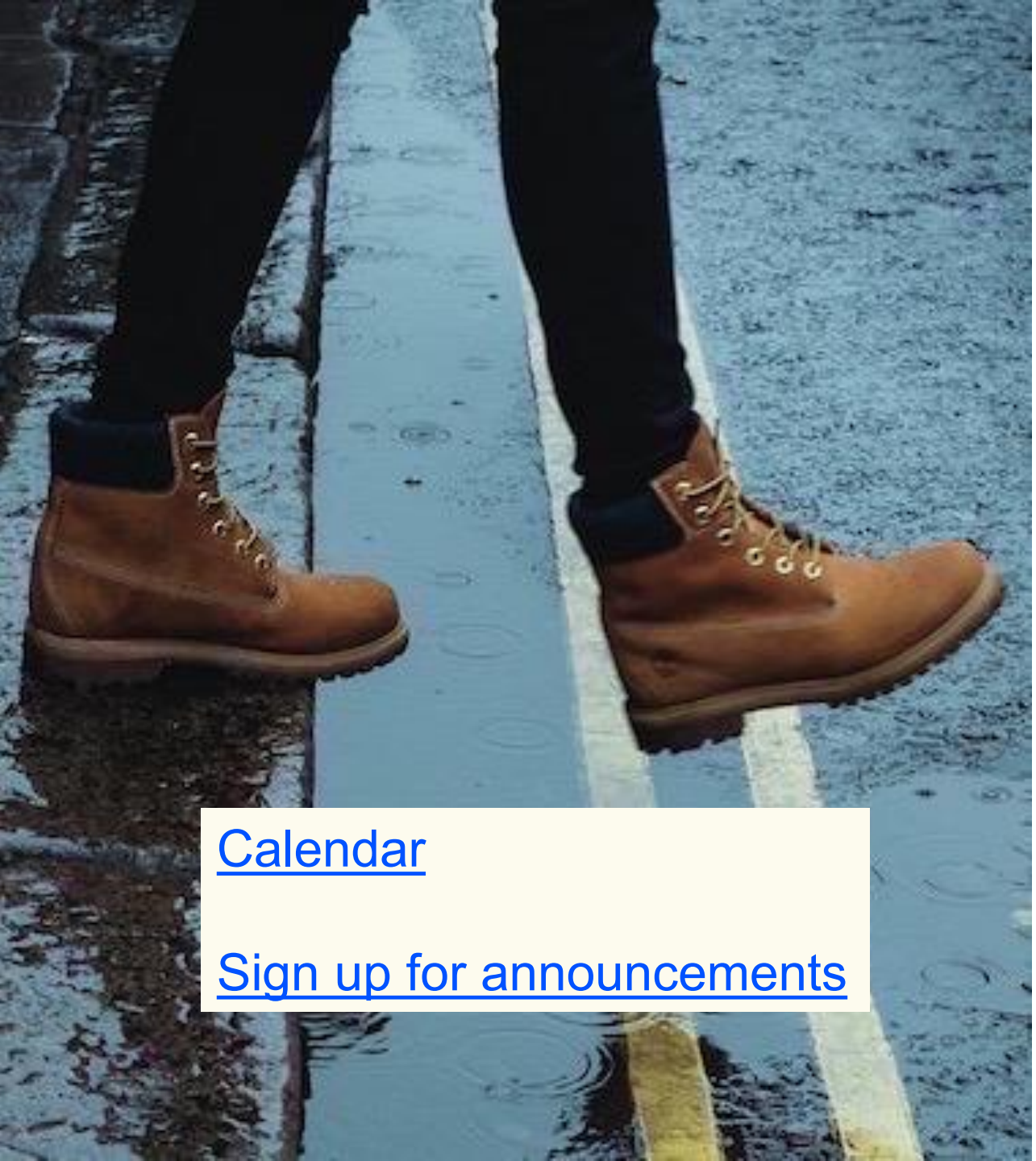
Next

Feedback:

Please fill out our feedback form

https://forms.gle/metB3BtKAbgbPar2A

AlphaPlus



Calendar

Sign up for announcements

Next at AlphaPlus

Workshop Series (Wednesdays 3:30 – 5:00)

- Inclusive Learning: November 18, 25, December 2
- TBA: January 13, 20, 27
- Canvas: February 24, and March 3, 10

Lunch and Learn (Tuesdays 12:30 – 1:00)

- November 3
- January 5
- February 9

AlphaPlus

Thank you

Guylaine Vinet
gvinet@alphaplus.ca
alphaplus.ca
416-322-1012 x 121
1-800-788-1120 x 121

Tracey Mollins
tmollins@alphaplus.ca
alphaplus.ca
416-322-1012 x 108
1-800-788-1120 x 108



AlphaPlus

Image credits



Photo by Franck on Unsplash



Photo by Franck on Unsplash



Photo by Clem Onojeghuo on Unsplash

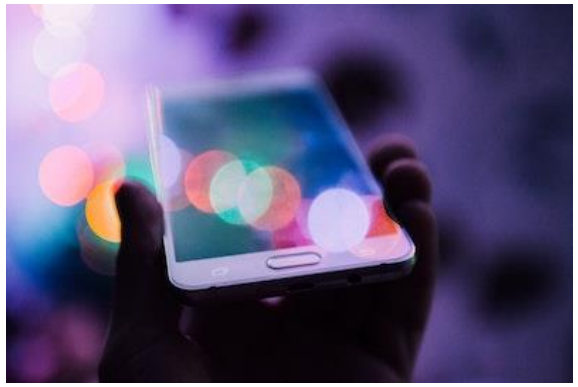


Photo by Rodion Kutsaev on Unsplash



Photo by Wes Hicks on Unsplash