CHINOOK ARCH
REGIONAL
LIBRARY SYSTEM

ONLINE **PRIVACY**

CLASS 2 OF 7 IN THE FUNDAMENTAL DIGITAL LITERACY SKILLS PROGRAM

TABLE OF **CONTENTS**

INTRODUCTION

The Internet is a wonderful thing: it allows us to connect instantly with loved ones living thousands of miles away, watch more films than we knew existed, take care of important financial decisions, and even shop for groceries! However, with this great connectivity comes some risk. Every time we go online, we put our personal information, our data, at risk - and there is no way to be 100% protected. The purpose of undertaking online privacy and security measures is to minimize the risks we face. It is like when we get behind the wheel of a car, or catch a bus: we accept there are risks with driving, but we do everything we can to avoid them.

Chinook Arch Regional Library System and the Government of Canada believe that the fear of what might happen to you online should not keep you from exploring the Internet. In fact, with so many important (or just fun) activities moving online it might soon be impossible to remain completely disconnected. We hope that this class and accompanying guide help to relieve some of your worries and provide you with some helpful ideas for practicing digital hygiene, the small actions you can take to minimize the risks to your information and identity. With this knowledge, we hope that you build your confidence in digital literacy and explore more of the digital world.

We would like to thank the creators of the *Protecting Your Online Privacy* guide, which provided a lot of the information in this booklet about privacy and security, data, self-assessment, and privacy technologies.

FUNDAMENTAL DIGITAL LITERACY SKILLS PROGRAM
PROUDLY PRESENTED BY

CHINOOK ARCH REGIONAL LIBRARY SYSTEM

With funding from
Canada

PRIVACY OR SECURITY?

PRIVACY

safeguarding your identity and online activity

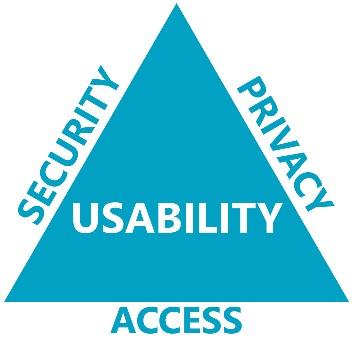
SECURITY

safeguarding your data (all of those pieces of personal information)

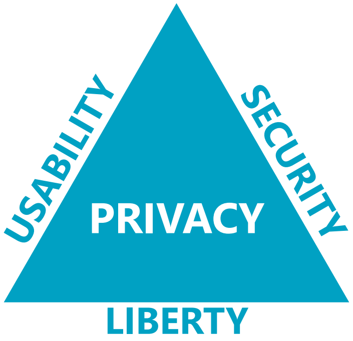
There is considerable overlap between the two, and their differences can get incredibly complex. Aspects of your user identity make up your secure data, and should be protected with stronger security measures.

Think about hospitals and clinics: they use secure systems to contact you about your test results, usually by asking you to come in person, and no one else has access to your personal information - unless you give permission. There is very little movement of information. Hospitals and clinics also have privacy provisions: you have access to some information, like your doctor's business phone number, but not their home one. You may also only be able to access information at certain times.

Keep in mind that both privacy and security affect your computer's **USABILITY**: since there needs to be some exchange of information between your computer and the Internet, if you make your privacy protections too strong you might not have easy access to the Internet



Your personal privacy comfort level is a careful balance between your liberty online, and your desired levels of security and usability.



Your browser fingerprint is a collection of unique online information (browser, operating system, name, etc.) that you leave behind on every site you visit, and can be captured by these websites. This information might then be tracked or sold.

WHAT DATA YOU HAVE AND WHO WANTS IT

What personal information makes up your data that you want to keep safe?

- Name, phone number, address
- Birthdate, birth place, family names
- Bank information, Social Insurance Number, tax filings
- Health and medical information (including family history)
- Shopping history and habits
- Public posts, including comments on news articles and online forums
- Location, where you've checked in (ie: posting what hotel you're staying at), how much time you spend there
- Your social networks, IDs, followers, and who you follow

It's a good idea to make your PERSONAL PRIVACY TRIGGERS list - the information you'd like to protect or at least prefer not to share openly. Think broadly.

Who might want your private data?

- Advertisers
- Data brokers, people who collect your data from websites to build profiles of you to sell
- Former partners, friends, and relatives who might be quite innocent in their snooping into your life, but who also might be trying to make trouble
- Your current or future employer
- Large corporate and government entities
- Hackers

ONLINE **RISKS**

Below are some of the major risks you will face when you go onto the Internet. While these risks sound frightening, don't let them stop you from exploring the Internet. Being aware of them will make you safer.

SOCIAL ENGINEERING

This is the human element – people who will use deception to ask you for your personal and/or confidential information by exploiting familiarity, creating a hostile situation, or gathering information about you. Usually this information is asked for in person, like over the phone. Know what information you can give out depending on the situation, and also know how legitimate organizations will ask for that information.

MALWARE

This is a type of harmful program that is installed on your computer, often without your permission or knowledge. Some types of malware include worms, Trojans, adware, and spyware, and they can be profitable for criminals. They often come attached to downloads, so be careful and make sure you asked for that download.

SCAREWARE

These are scary pop-ups that appear when you visit a website telling you your computer is infected and that you need to 'click here' to remove the virus. They are usually infected with malware, often a Trojan program that allows 'ratting' – a remote access Trojan program that people use to get inside your computer and control it. They can even turn your computer camera on without letting you know. If you get one of these pop-ups, don't click on it – not even the X to close! Use the Ctrl + Alt + F4 keystrokes to close it.

PHISHING

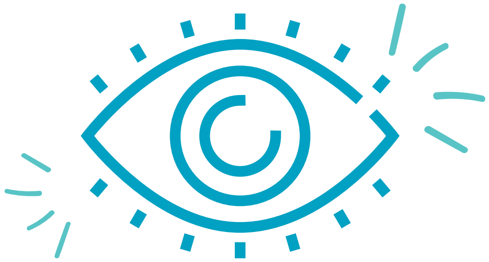
Phishing is an attempt to get sensitive information by pretending to be from a trustworthy source or organization, or a legitimate request for information. These attempts usually come as an email, so ask yourself some questions: do you recognize the sender; does it seem out of character; does it make you uncomfortable. Do not respond to them unless you are certain it is legitimate.

COOKIES

These are small bits of data that websites store on your computer that allow them to remember you and your preferences, but also track you and build data profiles. You will usually be asked to accept the cookies as soon as you get to a website, and they can improve the site's usability. Content blockers can detect and block cookies, and you can always delete them in your browser settings.

PUBLIC WI-FI

While using public Wi-Fi connections is not a risk as such, it is important to understand that these open services can be intercepted, have poorer security, and be more likely to gather and sell your data.



PRIVACY SELF-ASSESSMENT

If you are concerned (or even just curious) about your current privacy management, there are a few quick tools you can use to assess.

DOX YOURSELF

"Doxxing" means someone sets out to publish someone else's personal identifying information online, like their home address and phone number, and it's usually done with malicious intent. Much of the information needed for such actions is easily found online. If you're concerned about what information can be found about you, Google your name in quotations ("John Smith") and see what information is revealed, and what sites it's on. Likewise, try this with your email address(es).

CHECK IF YOU'VE BEEN PWNED

Pwning means your email address/username, and possibly passwords have been exposed in online data breaches. The older your email address is, the more likely it's been breached. Go to the website https://haveibeenpwned.com/ and enter your email address(es) into the search bar. If your addresses bring up results, don't panic! Check the dates of these data breaches and think about the last time you were at that website: have you since changed your password or registered for a new account?

DO A SECURITY AUDIT OF YOUR SOCIAL MEDIA ACCOUNTS

For each social media site you have an account with (Facebook, Twitter, etc.) go to your user account settings to check your privacy and security settings. It's a good idea to do this once or twice a year, just in case the website has reset them to the default.

CHECK YOUR INTERNET BROWSER'S PRIVACY PROTECTIONS

While you're on your chosen Internet browser (like Google Chrome), go to the website https://panopticlick.eff.org/ and click the TEST ME button. The site will conduct some quick tests to see how well your browser keeps your information private. If you're unhappy with the results, look into installing some privacy tools.

PRIVACY TECHNOLOGIES

Every time you visit a web site, your computer and that site exchange information in order to make the Internet more usable. This communication makes you uniquely identifiable through your browser fingerprint. You want to reduce, not remove, your browser fingerprint; removing it entirely is difficult and can make popular websites function poorly (sometimes even breaking them).

ENCRYPTION

Symmetric encryption is a simple form of encryption used on personal devices. You can do this by making sure you have to enter a password or passcode when you turn on or unlock your device. This master password means that even if your hard drive or memory is removed, your device is still safe if your password is secret. Some mobile devices use biometric encryption (fingerprints or facial recognition).

VPN

A VPN is a virtual private network, a software program that sets up a secure, encrypted Internet connection. They hide a lot of information about what you're doing online, and mislead any geo-tracking software that websites use – meaning you might be accessing the Internet at your home in Canada, but your VPN makes it look like you're in the United States. If you decide to use a VPN, make sure it's one that you pay for.

PASSWORD MANAGERS

We all have way more online accounts than we have creative passwords for – this is usually why many of us end up using the same password for everything! However, that's like leaving the key to your house in the lock: once it's exposed, malicious agents can get into everything. Instead, it's a good idea to install a password manager software on your computer that will remember your login information. This will take the pressure off you, and you also won't have to remember where you wrote it down. Don't allow your Internet browser to remember your passwords: if your Internet access is compromised, this information is easy to grab. A password manager stores your information in a separate place on your computer. LastPass (**https://www.lastpass.com/**) and 1Password (**https://1password.com/**) are both excellent options, and the free version of LastPass is adequate for the average Internet user.

ANTI-VIRUS SOFTWARE

Some people in the IT field believe that installing anti-virus software is more dangerous than it's worth: full protection often means giving the program access to your private passwords, so hackers only need to attack the software to get your information. Furthermore, many programs can be free, which means they likely collect your data for their own purposes and share some of that data to make money. If you choose to install an anti-virus software, make sure you read the manual to know how much information it will collect.

PASSWORDS

Once you have set up individual passwords for your various accounts and installed a password manager – if you want one – there are a few other actions to can take to ensure their security.

When creating your passwords, think of the *Star Wars* character Chewbacca:

- **Make it unique**
- **Make it memorable**
- **Make it strong**
- **Make it long**

Try not to use any information about yourself as a password phrase that can be discovered relatively easily, like your mother's maiden name. The same goes for any security questions an account asks for – stick to less obvious answers, or even put false ones down (as long as you can remember them!).

Also, consider using stronger, more complicated passwords for more important accounts like your online banking.

KEEP IT SECRET

KEEP IT SAFE

ONLINE PRIVACY, SAFETY, AND CHILDREN

Children face many of the same risks that adults do online, and are especially at risk of cyber bullying. If you are a parent or guardian, make sure they are aware of the risks and, depending on their age, monitor their Internet usage.

WHAT ARE THEY DOING ONLINE?

ONLINE GAMING

VIDEOS (sharing and streaming)

CAMERAS (video chatting, uploading photographs)

SEARCH ENGINES AND WEBSITES

APPS (gaming, social media and networking, instant messaging)

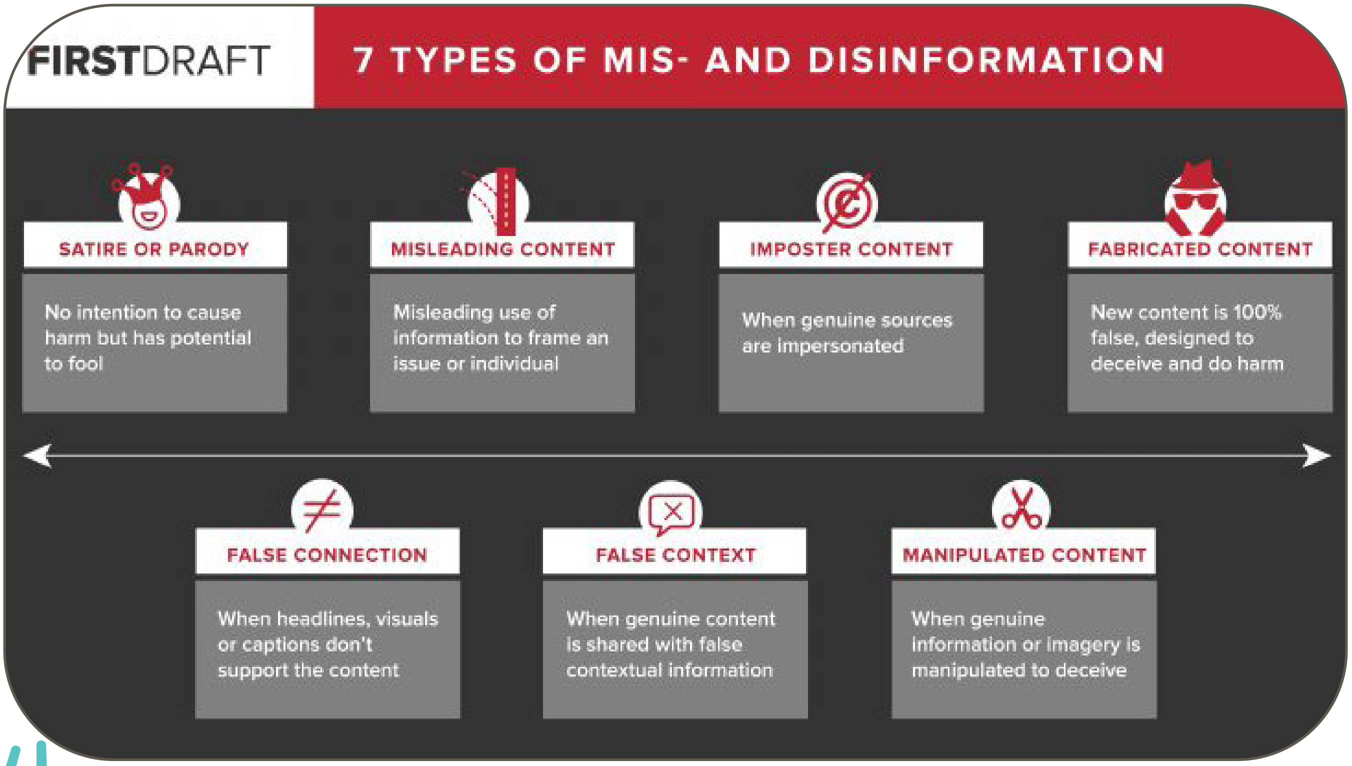
ONLINE PRIVACY, SAFETY, AND CHILDREN

HOW CAN YOU PROTECT THEM?

- Talk to them! Not only make them aware of the risks outlined in this guide and cyber bullying, but make sure they know they can come talk to you if they have questions
- If they are younger, make sure they know to ask for your permission before posting a photograph or any personal information
- Check the sites and games they visit to ensure they have privacy protections
  - Make sure they also have a way to report inappropriate behaviour
- Depending on your child's age, set their usernames and passwords yourself so you can access their accounts
- Teach them not to click on ads that appear on websites or games
- Use parental filters and controls on your Internet browser and devices
- Depending on their age, do an Internet search with them so you can see what results they see
- Set screen time limits
- Model appropriate use of content-sharing sites – ask their permission before posting their photo, so they know to ask you when they want to do the same
- Make sure apps are being downloaded from legitimate sites and stores (iTunes, Google Play)
  - Ensure these apps require parental permission for in-app purchases
- Discuss cyber bullying, how it looks, and how it can affect their lives
- Reinforce the idea that there is no true privacy on the Internet, so they should be wary of what they say and post
  - Once something is out on the Internet, it cannot be taken off even by deleting

IDENTIFYING **MIS- AND DISINFORMATION**

There is a lot of information found on the Internet, and, obviously, not all of it is correct. This type of information runs along a spectrum from satire and parody to manipulated content.



FIRSTDRAFT

7 TYPES OF MIS- AND DISINFORMATION

SATIRE OR PARODY

No intention to cause harm but has potential to fool

MISLEADING CONTENT

Misleading use of information to frame an issue or individual

IMPOSTER CONTENT

When genuine sources are impersonated

FABRICATED CONTENT

New content is 100% false, designed to deceive and do harm

FALSE CONNECTION

When headlines, visuals or captions don't support the content

FALSE CONTEXT

When genuine content is shared with false contextual information

MANIPULATED CONTENT

When genuine information or imagery is manipulated to deceive

Of course, there is incorrect information online that was put there accidentally or unknowingly. Not all the misinformation you will come across is on purpose!

If you are unsure about a news article, or anything you read online, there are steps you can take to check its validity - the first one is to check the source. Where did you read this information? Who sent it to you? These sorts of questions are important not only for judging the deliberate accuracy of information, but also to help us identify "fake news".

FAKE NEWS

According to the Thompson Rivers University Library, fake new is a type of hoax or deliberate spread of incorrect information with the intent to mislead for financial and/or political gain. The amount of information we consume every day - and the speed with which we consume it - means we run the risk of believing fake news, and skewing our perspectives on issues.

IT IS FACTUALLY INACCURATE

IT IS EASY TO CREATE, SPREADS RAPIDLY, AND IS EASILY CONSUMED

IT USES OUR EMOTIONS TO DISTORT FACTS, PREYING ON OUR BIASES

There are various reasons people fall for fake news: there is a growing decline in trust for the media and governments; creation of new content can be done without editing and fact checking; content is collected into a single "news feed" on social media platforms, mixed in with family and friends' updates; and, most importantly, fake news often appeals to our emotions about issues.

Our biases also affect our susceptibility to fake news, so it is important that we keep them in mind as we consume information. Implicit biases are our unconscious attitudes and/or stereotypes that we use to sort people into groups, while confirmation bias is our tendency to search for and interpret information that confirms our beliefs. The media also has biases, which are important to keep in mind.

HOW TO SPOT FAKE NEWS

CONSIDER THE SOURCE

READ BEYOND THE HEADLINE

CHECK THE AUTHOR

CHECK FOR SUPPORTING SOURCES

CHECK THE DATE

RESEARCH THE SITE TO MAKE SURE IT ISN'T SATIRE

CHECK YOUR OWN BIASES

CHECK WITH AN EXPERT OR FACT-CHECKER

Remember: disagreeing with an article does not make it fake news.

Test your ability to identify fake news
Go to mediasmarts.ca/quiz/break-fake-news "Fake News Quiz" section Option 1 (University of Akron)

CYBER HYGIENE TIPS

1. Stay on top of your operating system and security updates
2. Install or turn on your firewalls and pop-up blockers
3. Keep your privacy settings turned on
4. If in doubt, throw it out

- Hover your cursor over the sender's name on an email to see the full details of where it came from
- Do the same with a hyperlink in the email before following it
- Did it come to the wrong account?
- Are there spelling and grammar errors?

5. Don't click on or open any unfamiliar emails or pop-ups
6. If you get an attachment or a pop-up asking you to download something, ask yourself if you went looking for it
7. Be skeptical of everyone and everything on the Internet

- ie. if your browser warns you that a site you want to visit may be malicious, ask yourself if you have the right address

8. Be wary of free software or apps – they usually make their money from collecting data about you
9. Back up your files
10. Limit the personal information you provide to online accounts
11. Log off accounts before you leave
12. Be aware of what you post online

- Including text and online messaging services

13. Cover your laptop camera with tape (especially if kids are using the computer)
14. Only give secure sites your information (look for a padlock image or https at the start of the website URL)

- Consider using a private browser window (Incognito mode)
- Use a secure, privacy-focused search engine (DuckDuckGo)
- If you're just browsing the Internet, be wary of suspicious-looking sites

15. If you're using a public computer, be wary of anything plugged into the ports

RESOURCES

Online Privacy

- Protecting Your Online Privacy guide: https://drive.google.com/file/d/1OqoS7BSyTP4tk4axLXe_hH4KoLgOgZOQ/view
- Office of the Privacy Commissioner of Canada: https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/online-privacy/
- Government of Canada: https://www.getcybersafe.gc.ca/index-en.aspx
- Surveillance Self Defence: https://ssd.eff.org/
- Privacy Tools: https://www.privacytools.io/

Protecting Your Children

- Childnet International: https://www.childnet.com/resources
- UK Safer Internet Centre: https://www.saferInternet.org.uk/
- Social media checklists: https://www.saferInternet.org.uk/advice-centre/teachers-and-school-staff/teaching-resources/social-media-checklists
- Canadian Centre for Child Protection: https://www.cybertip.ca/app/en/Internet_safety
- Protect Kids Online: https://protectkidsonline.ca/app/en/

Identifying Mis- and Disinformation

- First Draft graphic: https://firstdraftnews.org/fake-news-complicated/
- Media Smarts: https://mediasmarts.ca/break-fake
- Thompson Rivers University Library Guide: https://libguides.tru.ca/fakenews/
- Toronto Public Library: https://www.torontopubliclibrary.ca/spotfakenews/

Tools

- Privacy assessment: https://haveibeenpwned.com/
  https://panopticlick.eff.org/
- Password managers: https://www.lastpass.com
  https://1password.com/
- Fake news quiz: https://mediasmarts.ca/quiz/break-fake-news