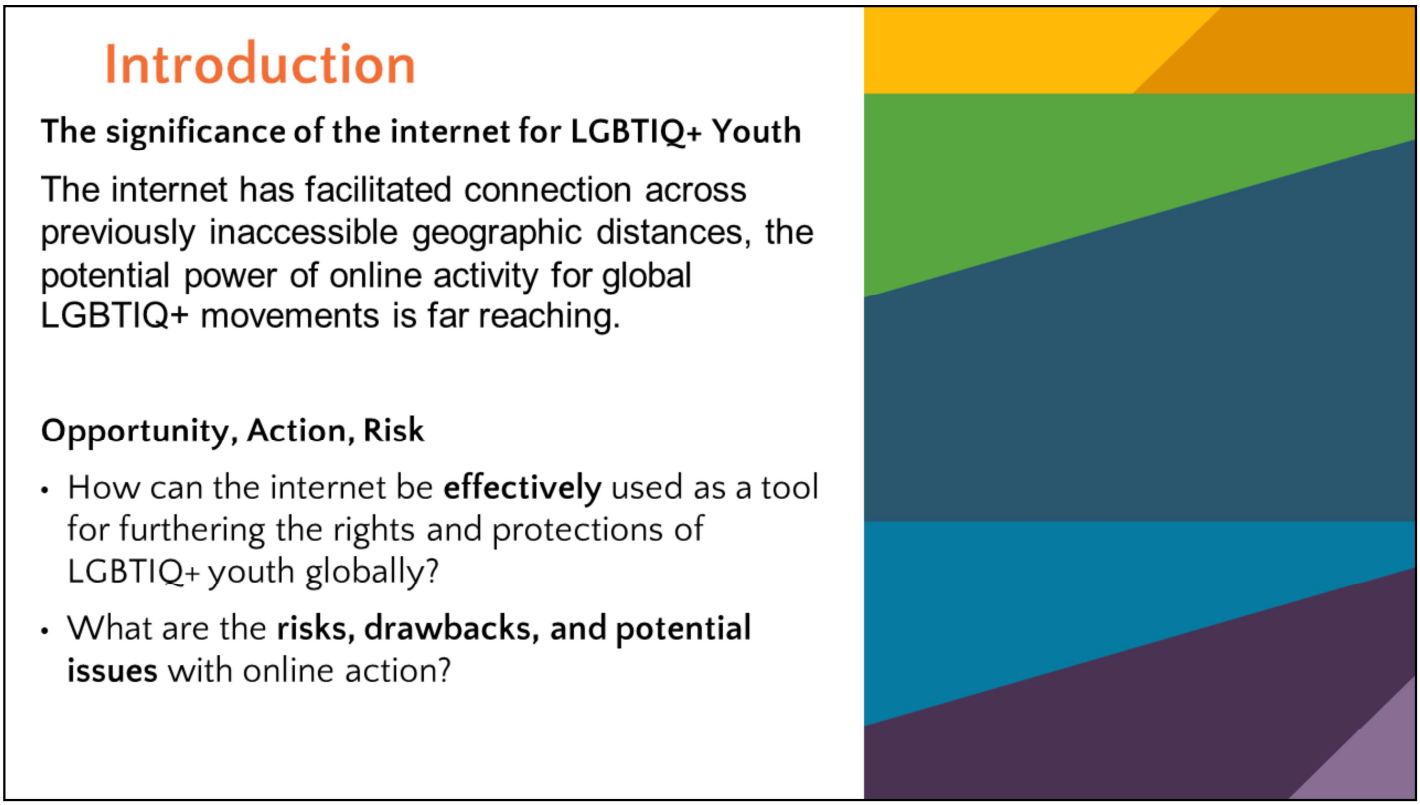
Queer Youth Dialogues

Stream 2: LGBTQI+ Youth Digital Security Training

GLOBAL QUEER YOUTH NETWORK

Introduction Points:

- This training will be the first session in digital security capacity building with a specific lens for the risks associated with working in the global issue area of LGBTIQ+ Youth Activism, Advocacy, Organizing, or intersectional support work.
- This training agenda has been set in response to the self-assessment surveys completed by our core group of participants
- Following this training we will be organizing and hosting “fireside chat” sessions where industry experts will be invited to casually discuss their field, speak to the concerns of this group, and make practical recommendations.



Introduction Continued:

- The significance of the internet for LGBTIQ+ Youth cannot be understated. The UN Sustainable Development Goal 9: *Build resilient infrastructure, promote sustainable industrialization and foster innovation* directly speaks to the importance of equity and safety in engaging with technology. The 2030 Agenda recognizes the need to develop knowledge societies where everyone has opportunities to learn and engage with others, which starkly highlights the need for access to Information and Communication Technologies (ICTs).

- Particularly for LGBTIQ+ youth , many of whom are considered digital natives, the internet is a vital educational, community forming, and organising space. Young people growing up today are unlikely to recall a time before the internet, possibly even unable to recall atime before high-

speed mobile internet. For many young people, the Internet may not seem separate from everyday life, as it felt for those present in the Internet's emergent years.

- With an understanding of the internet's position as vital we must explore the realities of **Opportunity, Action, and Risk** associated with online activity
    - The aim of any cyber security strategy is to protect as many assets as possible and certainly the most important. Since it is not feasible or even sensible to try to protect everything in equal measure, it is important to identify what is valuable and needs greatest protection, identifying vulnerabilities, then to prioritise and to erect defence-in-depth architecture that ensures continuity.
        - https://medium.com/e-tech/the-abc-of-cyber-security-44b922e2c8c5

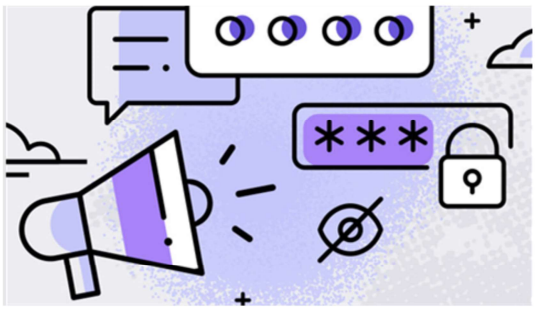
The agenda for today's session is as follows:

- An introduction to the session
- Overviewing Core Concepts such as Digital Footprints and core terminology – the digital footprint will have an interactive element
- Then we will move on to assessing risk, which will also bring a practical element
- After this we will explore some practical steps towards protecting yourself online
- Following this practical introduction we will then explore the idea of secure browsing, here we will overview some basic steps one can take to improve your security
- Finally we will go in-depth into some of the systems for the Queer Youth Dialogues
- Then the floor will be open for questions

Terminology

There are a few basic terms and ideas we must understand before taking any action:

- **Cookie**: Cookies are text files with small pieces of data — like a username and password — that are used to identify your computer as you use a computer network.
- **Cloud (computing/ storage)**: Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power.
- **Encryption**: The process of encoding data to prevent unauthorised access.
- **Firewall**: A defensive technology designed to suggest place a protective layer between your devices and the internet.

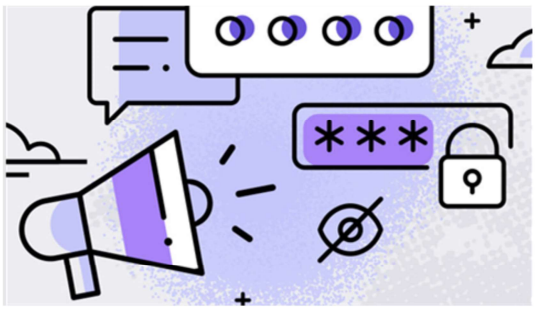


Before we can go much further it is vital that a few core words and phrases are understood

- **Cookie**: Data stored in a cookie is created by the server upon your connection. This data is labelled with an ID unique to you and your computer. When the cookie is exchanged between your computer and the network server, the server reads the ID and knows what information to specifically serve to you. When you visit a new webpage you likely are prompted to “agree to cookies”
- **Cloud**: Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term is generally used to describe data centres available to many users over the Internet (Google drive, OneDrive, Apple iCloud, DropBox)
- **Encryption**: The process of encoding data to prevent unauthorised access by ensuring the data can only be accessed with a key.
- **Firewall**: A defensive technology designed to suggest place a protective layer between your devices (phone/tablet/computer) and the internet. Only allowing trusted traffic through the firewall. Firewalls can be hardware or software based.

Terminology Continued

- **IP Address:** An internet version of a home address for your computer.
- **Personalisation Ads**: Enabled by the sharing of cookies across platforms and service providers.
- **Two Factor Authentication (2FA)**: Multi-factor authentication is an electronic authentication method in which a user is granted access to a website only after successfully presenting two or more pieces of evidence to an authentication mechanism.
- **Virtual Private Network (VPN):** A tool that allows the user to remain anonymous while using the internet by masking the location (IP) and encrypting traffic.



- **IP Address:** An internet version of a home address for your computer, which is identified when it communicates over a network; For example, connecting to the internet (a network of networks).
- **Personalisation Ads**: Enabled by the sharing of cookies across platforms and service providers. Enabling these personalisation permissions allows applications and providers to have access to your data to varied degrees, consider this a form of surveillance.
- **Two Factor Authentication (2FA)**: Multi-factor authentication is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism.
- **Virtual Private Network (VPN):** A tool that allows the user to remain anonymous while using the internet by masking the location (IP) and encrypting traffic.

Core Concept: Digital Footprint

What is your Digital Footprint?

A digital footprint is data that is left behind when users have been online. There are two types of digital footprints which are passive and active.

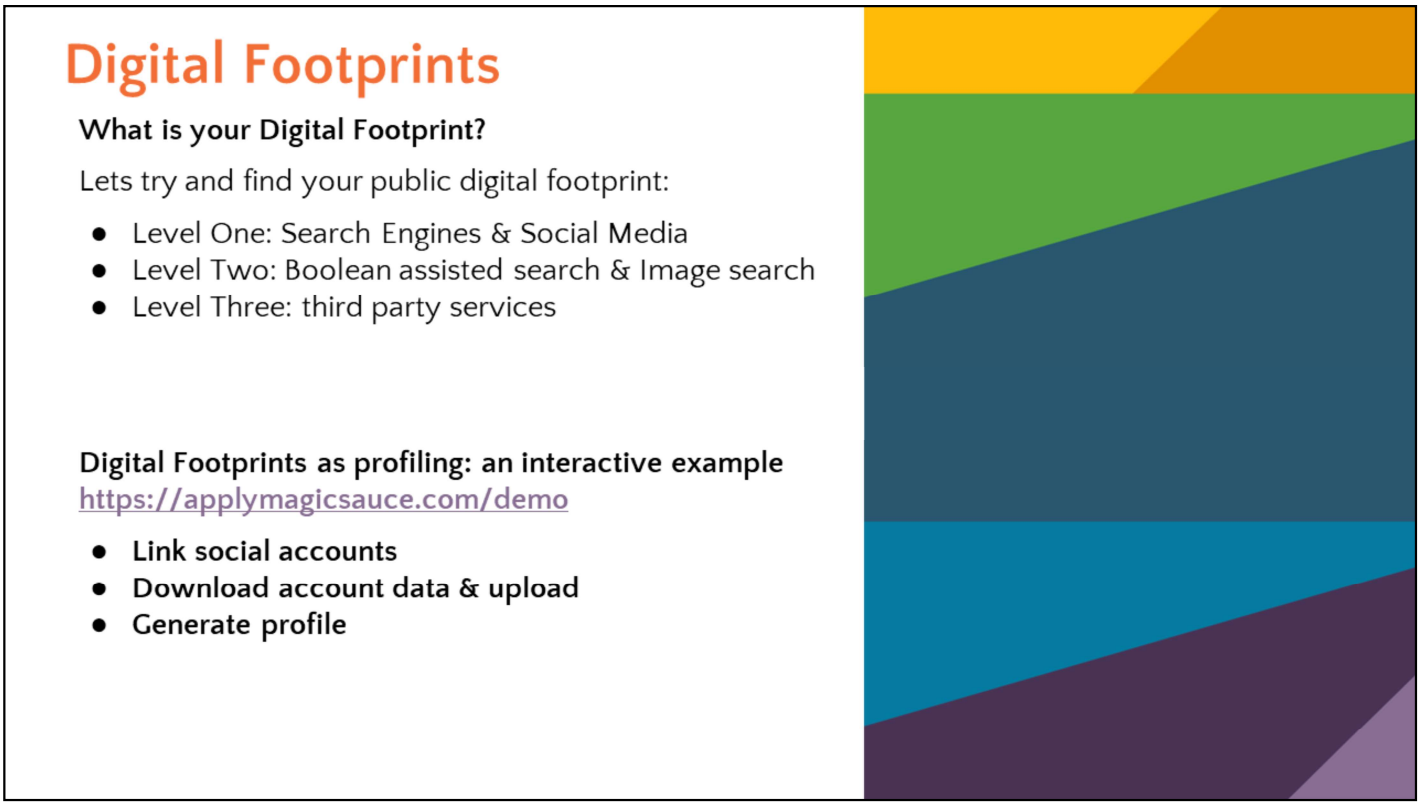
A passive footprint is made when information is collected from the user without the person knowing this is happening.

An active digital footprint is where the user has deliberately shared information about themselves either by using social media sites or by using websites.

- Much like the concept of a carbon footprint, your digital footprint is the culmination of the data you create and leave behind as you travel the internet.
- **Passive & Active digital footprints:**
- An example of a passive digital footprint would be where a user has been online and information has been stored on an online database. This can include where they came from, when the footprint was created and a user IP address. A footprint can also be analysed offline and can be stored in files

which an administrator can access. These would include information on what that machine might have been used for, but not who had performed the actions.

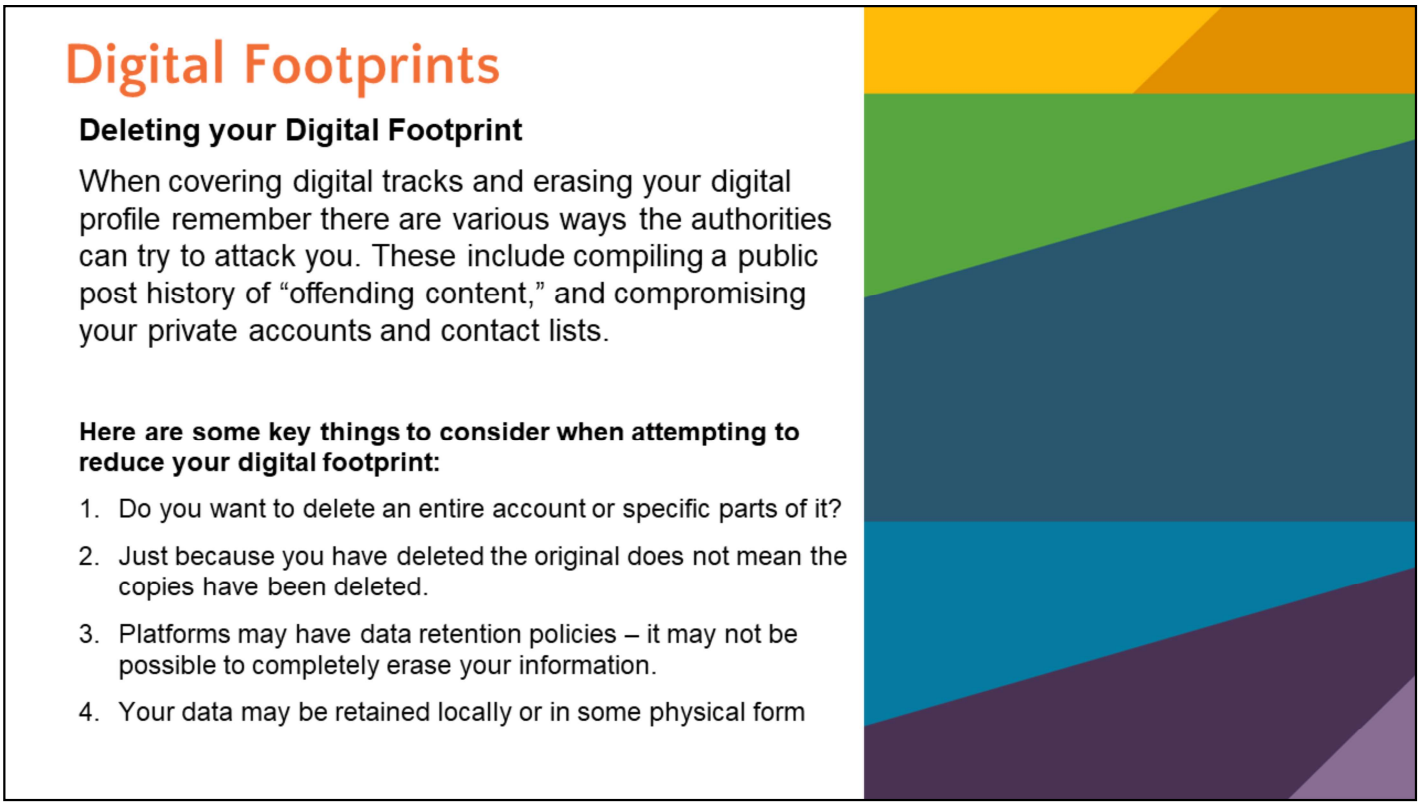
- An example of an active digital footprint is where a user might have logged into a site when editing or making comments such as on an online forum or a social media site. The registered name or profile can be linked to the posts that have been made and it is surprisingly easy to find out a lot about a person from the trails you leave behind.



How much can you find out about someone from some basic google searching?

I invite you now to use me as a test subject if you want to do some sleuthing, there are three suggested levels to carrying out this search: Using basic search engine terms and trawling social media, using more specific Boolean assisted search and image search, and finally using a third party service which searches in-depth.

What is the point of understanding your digital footprint? This interactive example may illuminate, here you can see that some basic data taken from two social media platforms and LinkedIn have come together to create a detailed psychological profile. Practically this could be used for marketing and advertising, predicting your actions, making assumptions about your political leanings and associations.



So how can you work on reducing your digital footprint?

Here are some key things to consider:

1. Do you want to delete an entire account or specific parts of it: for example, do you want to delete individual tweets or your whole Twitter account?
2. It's likely that when you delete individual posts or selected content, you'll miss something which could be copied somewhere else, like in the inbox of someone you sent an email to.
3. Even if you delete your entire account, in some cases platforms have data retention policies that archive the data for law enforcement or government purposes. Other data may have been screenshotted by the authorities already or stored by service providers and platforms. It may not be possible to completely erase your information.
4. Your data may be retained locally, on your laptop or mobile device, and

retrievable by law enforcement using special tools. This guide will not cover
topics such as completely removing all physical media.

Start with a list of what content and accounts you want to delete. Consider the broad
categories of where your information may be stored: 1) email, 2) social media, and 3)
chat applications. You may find it useful to search for your own name on search engines
in order to determine what information is publicly available. One way to recall where you
have accounts online would be to go through your saved passwords and to carefully
comb through the list there. Bottom line: be methodical and patient in your approach

https://www.humanrightsfirst.org/sites/default/files/How%20to%20Delete%20Your%20Digital%20History%20-%20Updated%208.20.21.pdf

Assessing Risk

The scope of potential risks when engaging with digital activism [or any online activity for that matter] is wide and creating a guide which covers every potential risk is unattainable. Instead we must consider every action as having potential risks, it is vital to weigh up the potential harm vs. the potential benefit.

The golden rule of Digital Security is the ABC risk assessment model:

A. **Assessing** the risk - *If I do X what are the potential risks (Y)?*

B. Using **best practices** to address the risk - *How is best to avoid or limit the impact of Y?*

C. **Conformity** for future action in this risk area - *How do we ensure that people doing X understand how to best avoid Y in the future?*

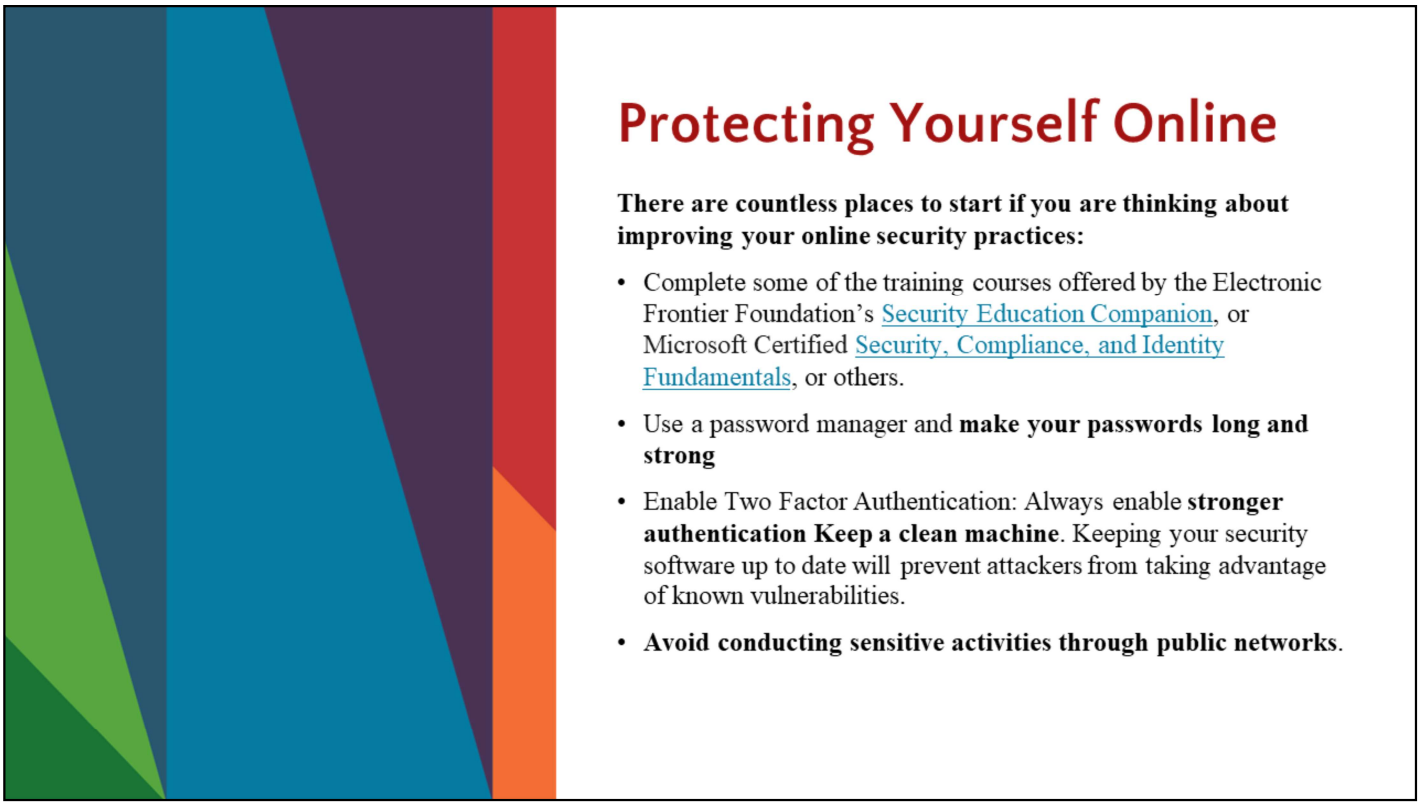
- Digital Security requires an individual consideration of risk and an understanding of the exchanges required to take certain steps to higher digital security [such as add-on compatibility in browsers]. The first step anyone should take in securing their online activity is to ensure your device has up to date antivirus software such as Kaspersky Security, AVG Antivirus, or McAfee. There are countless options which offer a variety of services and compatibility with mobile devices.
- The aim of any cyber security strategy is to protect as many assets as possible and certainly the most important. Since it is not feasible to try to protect everything in equal measure, it is important to identify what is valuable and needs greatest protection, identifying vulnerabilities, then to prioritise and to erect defence-in-depth architecture that ensures continuity. The Global Queer Youth Network is committed to developing strategic and sustainable digital security practices which improve protections for individuals and organisations.

Carrying out Risk Assessment – Example

Potential Action (X)	Risk (Y)	Mitigating Action	Notes
Accessing the internet	Location insecurity due to IP address being visible.	IP masking via Virtual Private Network (VPN) proxy servers.	There are many popular VPN providers such as ExpressVPN, NordVPN, Surfshark, CyberGhost.
	Device storage vulnerable	Install and use a well-rounded antivirus or device security application	Such as Kaspersky Security, AVG Antivirus, or McAfee.
Using an internet browser	Tracking across online activity	Tracker Blocking addons	https://www.eff.org/pages/cover-your-tracks
	Browser insecurity	Secure Browsing via Tor Onion browser	https://www.torproject.org/download/
	Data storage	Regular cookie deletion (you could set up automatic deletion)	Cookie autodelete extension for Chrome and Firefox
Communication Online (email)	Various possible angles of data insecurity or personal information deduction	Use secure email client hosting. Consider using different email accounts for different purposes. Regularly create new email accounts if the issue is personal data at risk.	https://riseup.net/en/email

As you can see on this slide, there are countless routes to take when you consider your online practices from a digital security lens.

Protecting Yourself Online



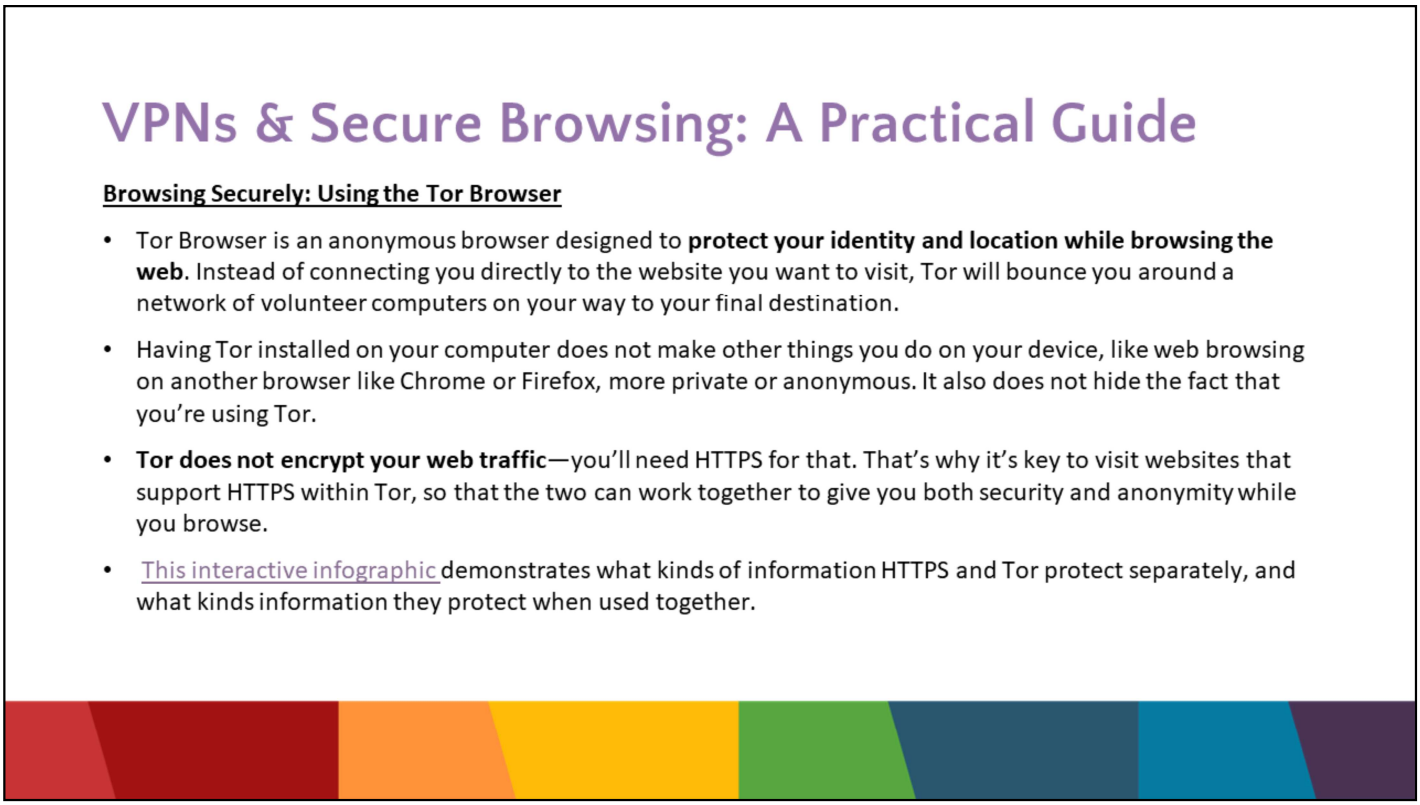
- Training Courses: it is always valuable to keep yourself upskilling in this area as it is constantly evolving.
- Password Managers: these tools will help you manage your various passwords and the autofill options will allow you to have more complicated passwords without concerns of forgetting them.
- 2FA: for an extra layer of security beyond the password that is available on most major email, social media and financial accounts.
- Keeping a clean machine: Update the security software, operating system, and web browser on all of your Internet-connected devices.
- Understand what wifi networks may be insecure for certain information: Avoid online shopping, banking, and sensitive work that requires passwords or credit card information while using public Wi-Fi.

VPNs & Secure Browsing: A Practical Guide

Browsing Securely: HTTP vs. HTTPS

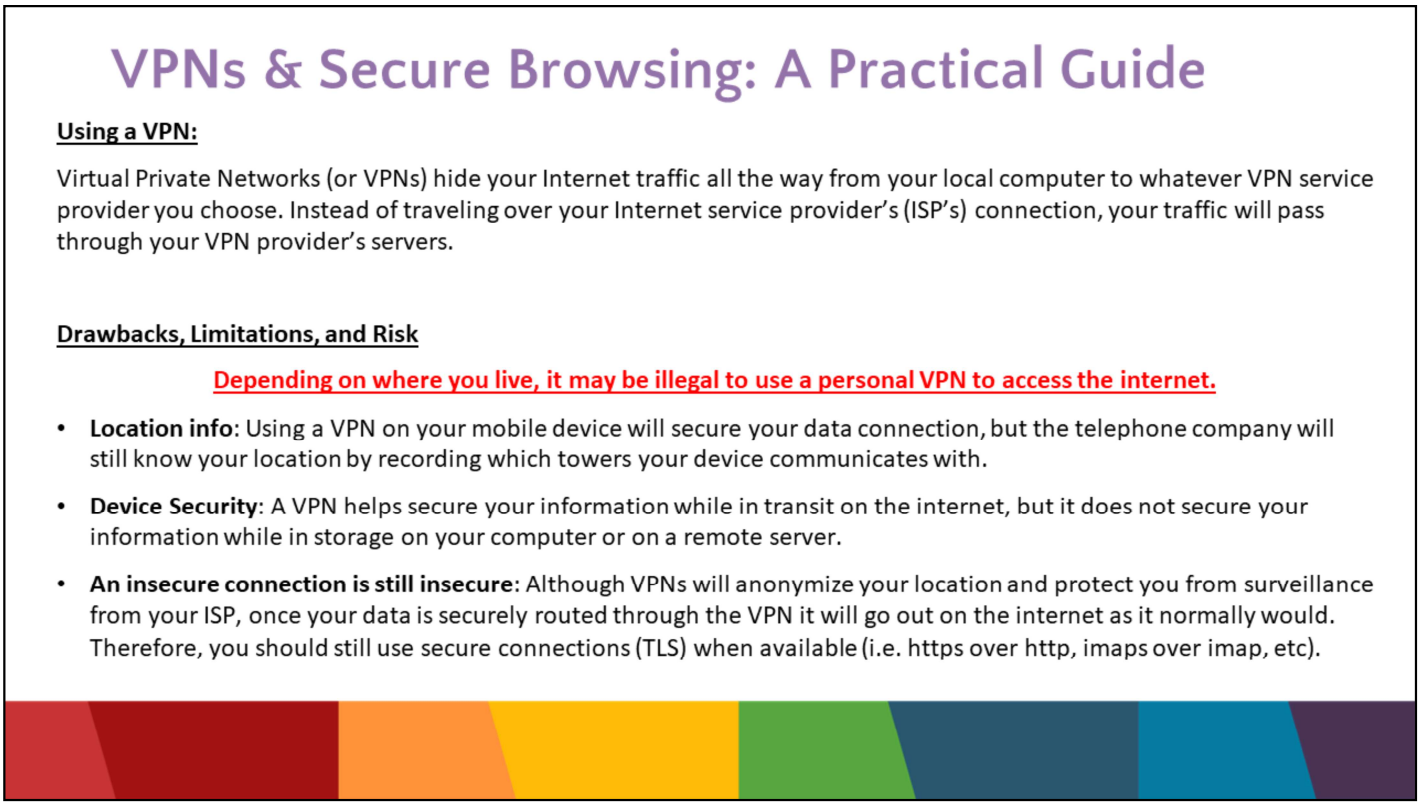
- There are two ways for a website to get to your browser: HTTP and HTTPS. The difference is that "S," which stands for "secure."
- When you see "https" and a little green lock next to the web page address in the top of your browser, that means you are using a secure connection.
  - For example, if you are using HTTPS to connect to www.eff.org/ssd, an eavesdropper can only see "www.eff.org". With HTTPS, an eavesdropper cannot see what part of a website you're visiting.

- The very beginning of any web browsing is the http or https part of a URL. What are these systems and why is it important to know the difference?
- Basically, the "S" in https stands for secure
- The web is in the middle of a large shift to using HTTPS for all webpages. This is because HTTP lacks any meaningful security, and HTTPS comes secure by default. Webpages that come to you over HTTP are vulnerable to eavesdropping, content injection, cookie and credentials stealing, targeted censorship, and other problems.
- When you see "https" and a little green lock next to the web page address in the top of your browser, that means you are using a secure connection. If someone is spying on the network and trying to see what websites users are visiting, an HTTP connection offers no protection. An HTTPS connection, on the other hand, hides which specific page on a website you navigate to—that is, everything "after the slash."



- So beyond Http and https how can you use internet browsers with some degree of security? Onion Browsing. Onion browsing is the name given to the TOR network and its internet browser.
    - Tor Browser is an anonymous browser designed to **protect your identity and location while browsing the web**. Instead of connecting you directly to the website you want to visit, Tor will bounce you around a network of volunteer computers (called "nodes") on your way to your final destination. This bouncing around **masks who you are and where you are connecting from**.

- Using Tor makes it harder for people monitoring you to know what you are doing online, and harder for people monitoring certain sites to know who is using them and where they are connecting from.
- It's important to remember that Tor will protect your privacy and anonymity only for activities inside Tor. Your web navigation may be anonymous, but it will be clear that you're using the Tor software.
- More information: https://www.eff.org/pages/tor-and-https



Using a VPN:

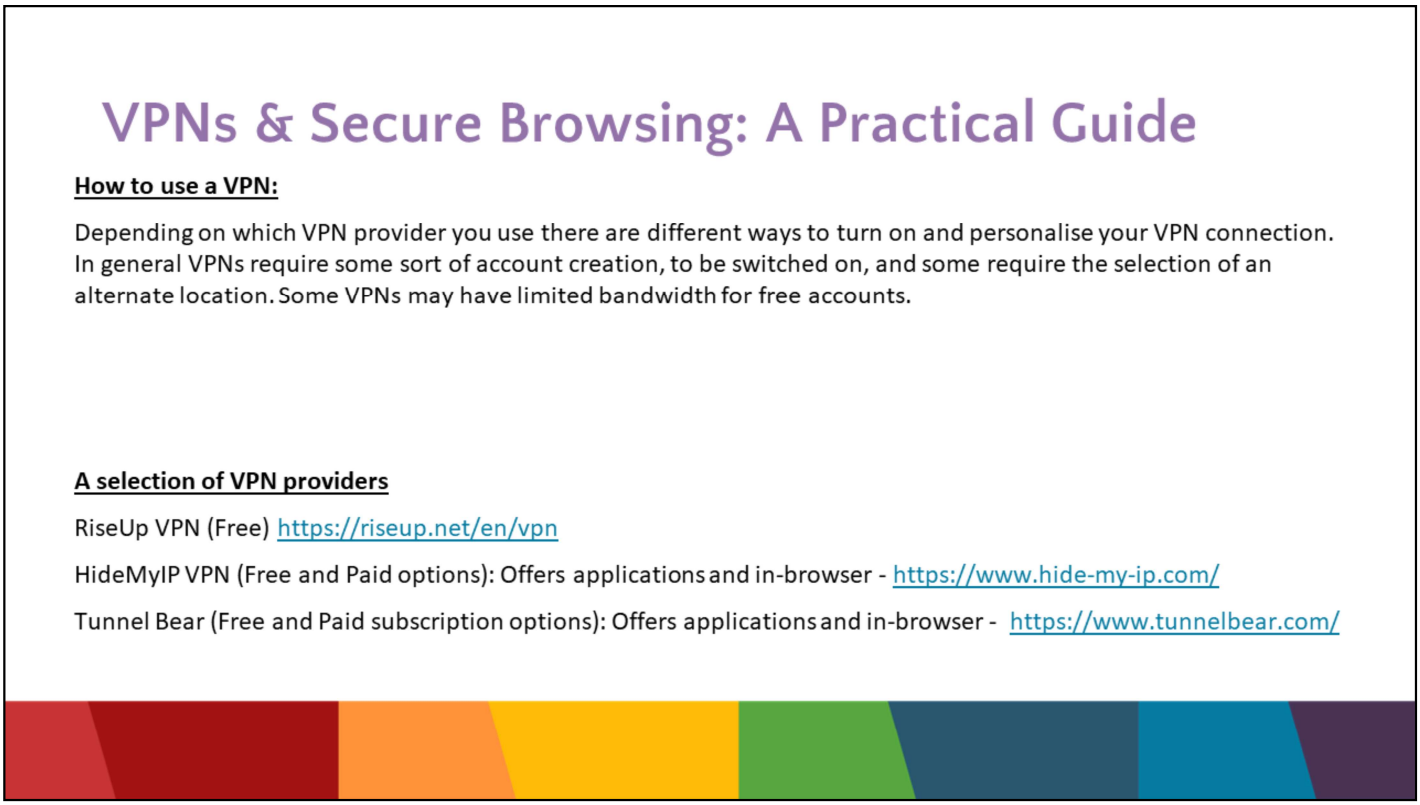
Virtual Private Networks (or VPNs) hide your Internet traffic all the way from your local computer to whatever VPN service provider you choose. Instead of traveling over your Internet service provider's (ISP's) connection, your traffic will pass through your VPN provider's servers. If someone is spying on your local network and trying to see what websites users are visiting, they will be able to see that you're connecting to a VPN, but will not be able to see what websites you are ultimately visiting.

VPNs are not a panacea: although VPNs accomplish a lot, they can't fix everything. For example, it cannot increase your security if your computer is already compromised with viruses or spyware. If you give personal information to a website, there is little that a VPN can do to maintain your anonymity with that website or its partners. For more information, see VPN anonymity.

Depending on where you live, it may be illegal to use a personal VPN to access the internet.

- China: Tightly Regulated
- Russia: Complete Ban
- Belarus: Complete Ban

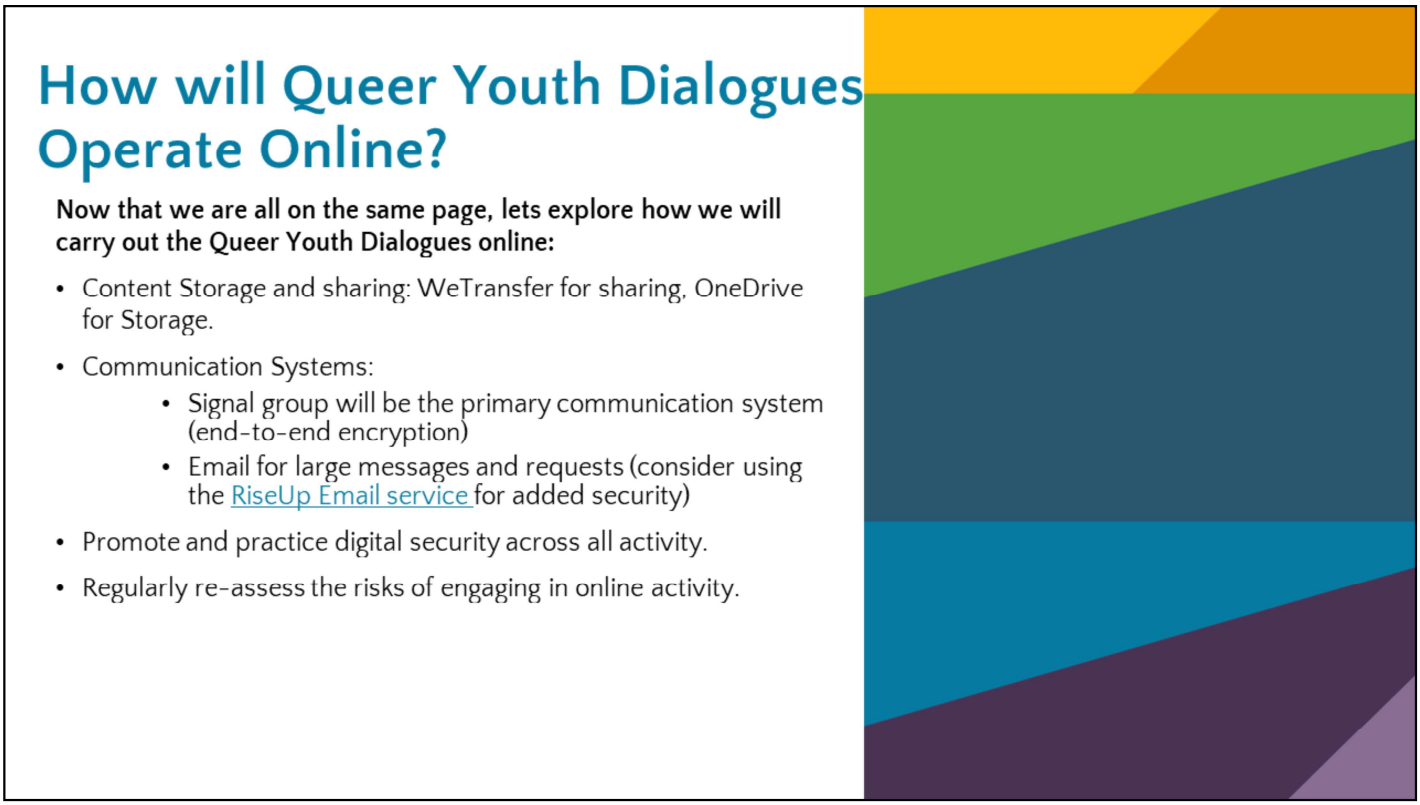
- North Korea: Complete Ban
- Turkmenistan: Complete Ban
- Uganda: Partially Blocked
- Iraq: Complete Ban
- Turkey: Complete Ban
- UAE: Tightly Regulated
- Oman: Complete Ban



How to use a VPN:

- Depending on which VPN provider you use there are different ways to turn on and personalise your VPN connection. In general VPNs require some sort of account creation, to be switched on, and some require the selection of an alternate location. Some VPNs may have limited bandwidth for free accounts.

- In-browser VPNs such as *HideMyIP: In-Browser* are operational in the specific browser they are installed on, and will not provide protection if you, for example, have two different browsers open such as Google Chrome and Mozilla Firefox and only have the VPN active in one.
- Downloadable VPN applications are operational across all internet traffic from the device they are enabled on.



- When we want to create, share, and make available some content from the Queer Youth Dialogues we will either share it over WeTransfer or OneDrive.
- As you know since you are already in our Signal group – we will primarily communicate there. We can also send files via Signal.
- If you are interested in more secure email communication you are welcome to set up an account with RiseUp
- Moving forward we will be sure to regularly check in on our various systems to be sure everyone is feeling confident

Resources

- Security Education Companion resources https://sec.eff.org
- Electronic Frontier Foundation https://www.eff.org/
- Download RiseUp VPN https://riseup.net/en/vpn
- Download Tor Browser https://www.torproject.org/
- Security toolkit, sorted by operating system: https://securityinabox.org/en/