

# Cybersecurity Basics

Phillip Schneider  
Digital Services Librarian  
Gail Borden Public Library



# Agenda

- What's a Virus?
- Antivirus Software
- Web Browsers
- Passwords
- Safe Internet Use
- Buying online
- Updating
- Privacy

# What's a Virus?

A decorative graphic consisting of several horizontal lines of varying lengths and colors (green and white) extending from the right side of the slide.

# What is a Virus?

A malicious set of code meant to harm you and/or your computer

## How can my computer become infected?

- Emails from infected computers
- Downloads
- Bad websites
- Clicking dangerous popups



# A Virus Can...

- Record your keyboard strokes (Spyware)
- Steal private information such as passwords, credit card numbers, etc. (Spyware)
- Hold your files hostage (Ransomware)

# A Virus Can...

- Move to your computer with nothing more than an internet connection (Worm)
- Masquerade as a normal program which then installs a virus (Trojan Horse)
- Cause your computer to malfunction, crash and become non-responsive (Malware)

# Antivirus Software

A decorative graphic consisting of several horizontal lines of varying lengths and colors (green and white) extending from the right side of the slide.

# Free Antivirus Software



Windows Defender





# Subscription Antivirus Software



Kaspersky: Top rated by most reviews!

Bitdefender Plus



**Bitdefender**<sup>®</sup>



**Norton**<sup>™</sup>  
by Symantec

Norton

McAfee



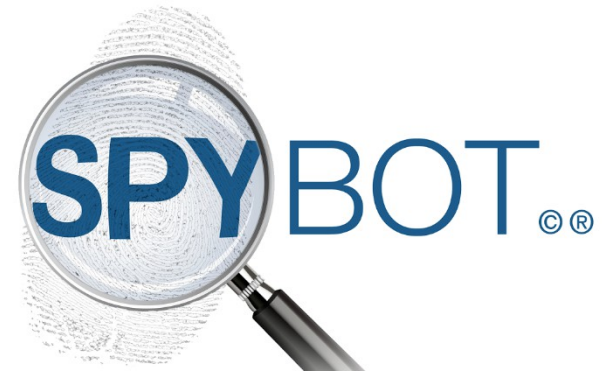
**McAfee**<sup>®</sup>

# Secondary Defense Software



Malwarebytes

Spybot



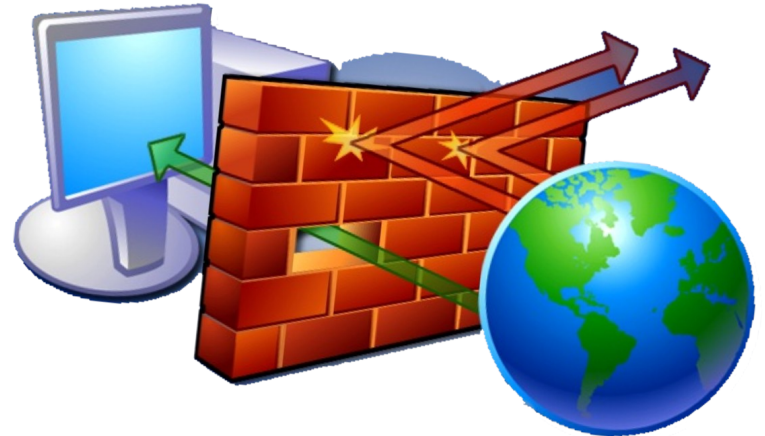
# Firewalls

## What is a Firewall?

A program that monitors and blocks bad traffic attempting to hack your computer.

## Do I have already have a Firewall?




- Windows Firewall
- A firewall is built into most paid antiviruses



# Web Browsers

A decorative graphic consisting of several horizontal lines of varying lengths and colors (green and white) extending from the left side of the slide towards the right, positioned below the main title.

# Safest Web Browsers

1. Google Chrome 
2. Fire Fox 
3. Windows Edge  & Safari (mac only) 
4. Opera 

# Browser Extensions for Privacy



Adblock Plus

Adblock  
Plus



Disconnect



**GHOSTERY**<sup>®</sup>

Ghostery



HTTPS Everywhere

# Passwords



# Passwords

## Create a Strong Password

- Use a minimum of 8 characters (longer is better)
- Use a long string of words
- Add numbers & symbols at the end (IE: !@#)\$)
- Use Upper and Lowercase letters

## 4Examp13:

- Thiswouldbegood74
- Ilovemycatfluffy7\$
- Lizardoceaniswavey8!

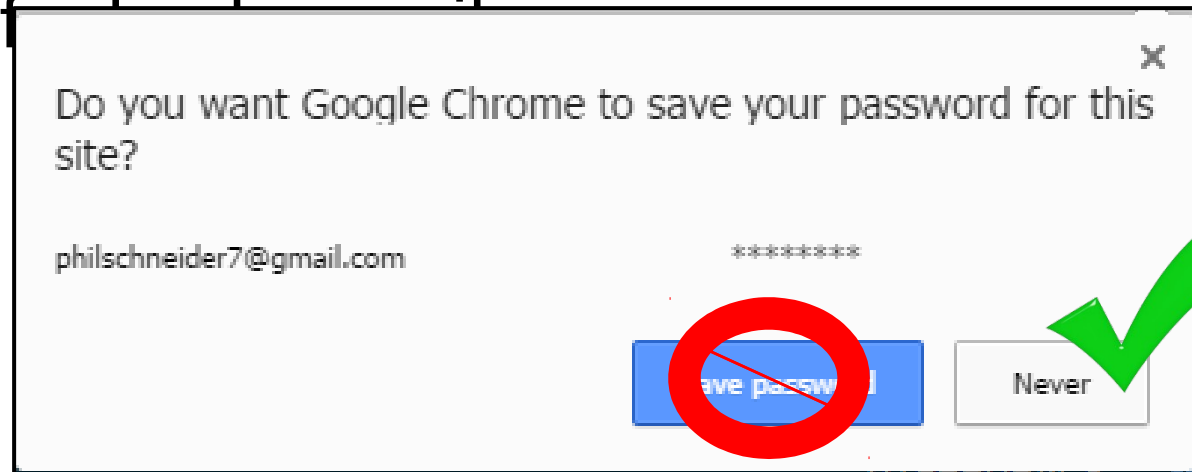




# Passwords

## Best Password Practices

- Never use the same password for multiple accounts
- Save your passwords on paper rather than on the computer
- Avoid letting your browser or programs save passwords



# Passwords

## Saving Passwords Safely with a Program

- Encrypts and protects your passwords on your mobile or desktop device
  - Is compatible with Android, IOS, Chrome, Firefox, and Safari
- Sticky Password
  - \$30 a year or \$150 for lifetime
- Keeper
  - Free version or \$30 a year
- True Key
  - Free version or \$20 a year

# Safe Internet Use



# Safe Internet Use

## Question to consider before proceeding

- Is this a well known site?
- Have I used this site safely before?
- Does this site make me feel uncomfortable?
- Is this site asking for things I don't want to share?
- Do I have a reason to trust this site?

# Safe Internet Use

- Do not click on popups
- Only give out private information to a trusted site
- Avoid clicking on strange links or advertisements
- If it sounds too good to be true it probably is

# Safe Internet Use

- Only download from official company websites

Bad site

The screenshot shows a search engine results page for the query 'avira'. The search bar at the top contains 'avira' and shows search filters like 'All', 'News', 'Shopping', 'Images', 'Videos', 'More', 'Settings', and 'Tools'. Below the search bar, it indicates 'About 13,900,000 results (0.66 seconds)'. The first result is an advertisement for 'Avira Antivirus Support - instant Help Call Toll Free No' with the URL 'www.speichereshop.com/Avira/products'. This result is highlighted with a red box and labeled 'Bad site'. The second result is an advertisement for 'Avira™ Antivirus 2017 Edition - Summer Sale - save 30% today' with the URL 'www.avira.com/Total-Security'. Below the advertisements, there are several organic search results, including 'Avira 2017 - Download free antivirus for PC & Mac' and 'Avira 2017 - Download free antivirus for PC & Mac'. These results are highlighted with a green box and labeled 'Official site'. On the right side of the screenshot, there is a snippet of the Avira Antivirus official website, also highlighted with a green box and labeled 'Official site'. This snippet includes the Avira logo, the text 'Avira Antivirus Software company', the website URL 'avira.com', and a brief description of the company as a German multinational security software company. It also lists technical support, headquarters, founder, and CEO information. At the bottom of the snippet, there are social media icons for Facebook, Twitter, LinkedIn, Google+, and Pinterest, and a section for 'People also search for'.

Official site

# Browser Blocking Tools



## The site's security certificate is not trusted!

You attempted to reach **192.168.17.129**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.

[Proceed anyway](#) [Back to safety](#)

[▶ Learn me understand](#)



## The site ahead contains harmful programs

Attackers on [www.bernbern.ch](#) might attempt to trick you into installing programs that harm your browsing experience (for example, by changing your homepage or showing extra ads on sites you visit).

Automatically report details of possible security incidents to Google. [Privacy policy](#)

[Details](#)

[Back to safety](#)



## Danger: Malware Ahead!

Google Chrome has blocked access to this page on [scores.espn.go.com](#).

Content from [us.bernverein.ch](#), a known malware distributor, has been inserted into this web page. Visiting this page now is very likely to infect your computer with malware.

Malware is malicious software that causes things like identity theft, financial loss, and permanent file deletion. [Learn more](#)

[Go back](#) [Advanced](#)

Improve malware detection by sending additional data to Google when I encounter warnings like this. [Privacy policy](#)



## Reported Unwanted Software Page!

This web page at [kat.cr](#) has been reported to contain unwanted software and has been blocked based on your security preferences.

Unwanted software pages try to install software that can be deceptive and affect your system in unexpected ways.

[Get me out of here!](#) [Why was this page blocked?](#)

[Ignore this warning](#)

# Safe Internet Use

## Google Transparency Report

[Home](#) [Traffic](#) [Requests to remove content](#) **[Security and privacy](#)**

[Requests for user information](#) **[Safe Browsing](#)** [Safer email](#) [HTTPS](#)

[Overview](#)

[Malware dashboard](#)

**[Site status](#)**

[Notes](#)

[FAQ](#)

### Safe Browsing Site Status

Google's Safe Browsing technology examines billions of URLs per day looking for unsafe websites. Every day, we discover thousands of new unsafe sites, many of which are legitimate websites that have been compromised. When we detect unsafe sites, we show warnings on Google Search and in web browsers. You can search to see whether a website is currently dangerous to visit.

Status of:



**Current status:** **Not dangerous**

Safe Browsing has not recently seen malicious content on www.gailborden.info.



# Safe Email Use

- Only click on links/download files from trusted emails
- Beware of hacked messages from “friends”
- Delete emails asking for personal information
- Google text of sketchy emails to check for scams
- Companies, like Microsoft, will never email or call you about problems with your computer

# Safe Email Use

FEDERAL TRADE COMMISSION ESPAÑOL

CONSUMER INFORMATION

[MONEY & CREDIT](#)

[HOMES & MORTGAGES](#)


[HEALTH & FITNESS](#)

[JOBS & MAKING MONEY](#)

[PRIVACY & IDENTITY](#)

[BLOG](#)

[VIDEO & MEDIA](#)

[SCAM ALERTS](#) 

[Vea esta página en español](#)

## SCAM ALERTS

what to know and do about scams in the news

Crooks use clever schemes to defraud millions of people every year. They often combine sophisticated technology with age-old tricks to get people to send money or give out personal information. They add new twists to old schemes and pressure people to make important decisions on the spot. One thing that never changes: they follow the headlines — and the money.

Stay a step ahead with the latest info and practical tips from the nation's consumer protection agency. Browse FTC scam alerts by topic or by most recent.

### Most Recent Scam Alerts

[Phony calls about health insurance](#)  
February 18, 2016

[Spread the word about government imposters](#)  
February 12, 2016

[Looking to get a high school diploma? Watch out for scams.](#)  
February 10, 2016

[Get Scam Alerts by Email](#)

### Browse Scams by Topic

- [Cars](#)
- [Charity](#)

# Safe Email Use

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

philschneider7@gmail.com

pwned?

Oh no — pwned!

Pwned on 2 [breached sites](#) and found no [pastes](#) ([subscribe](#) to search sensitive breaches)

- If you have been pwned change your password!

Desktop role-playing games website Roll20 suffered a data breach. Impacted by the breach and had email and IP addresses, names, bcrypt hashes, and digits of credit cards exposed. The data was provided to HIBP by a user identified as "JimScott.Sec@protonmail.com".

Compromised data: Email addresses, IP addresses, Names, Partial credit card data, Passwords



**Ticketfly:** In May 2018, the website for the ticket distribution service Ticketfly was defaced by an attacker and was subsequently taken offline. The attacker allegedly requested a ransom to share details of the vulnerability with Ticketfly but did not receive a reply and subsequently posted the breached data online to a publicly accessible location. The data included over 26 million unique email addresses along with names, physical addresses and phone numbers. Whilst there were no passwords in the publicly leaked data, Ticketfly later issued an incident update and stated that "It is possible, however, that hashed values of password credentials could have been accessed".

**Compromised data:** Email addresses, Names, Phone numbers, Physical addresses

- Is your email account secure after all the password breaches?  
Check it at <https://haveibeenpwned.com/>

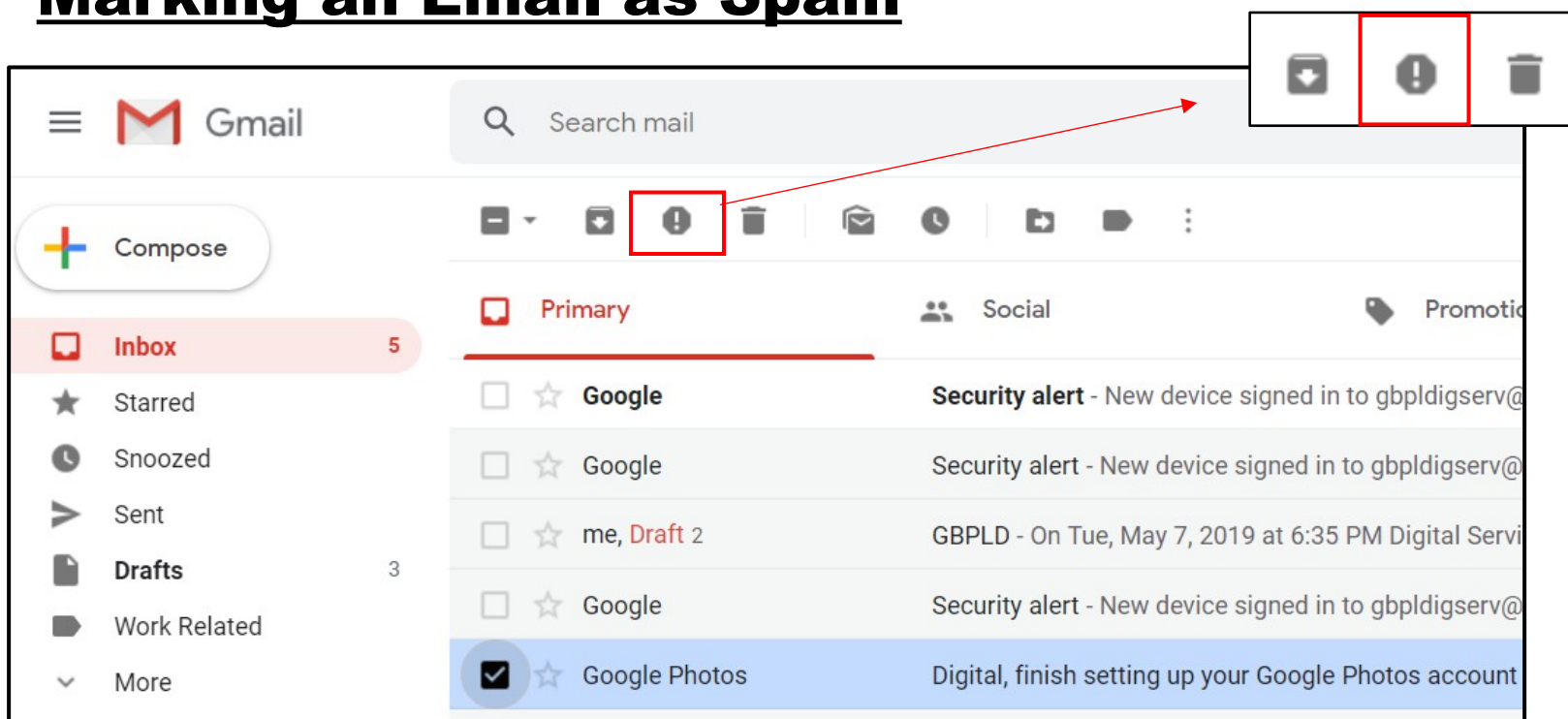
# 2-Step Verification

- Increases your security by texting you a code to access your account
- Greatly increases security of any account
- You know if your account was hacked right away



# Safe Email Use

## Marking an Email as Spam



1. Select the email
2. Mark it as spam

# Safe Email Use

## Spam Filters

### Settings



General Labels Inbox Accounts and Import **Filters and Blocked Addresses** Forwarding and POP/IMAP Add-ons Chat Advanced Offline Themes

The following filters are applied to all incoming mail:

Select: All, None

Export

Delete

Create a new filter Import filters

The following email addresses are blocked. Messages from these addresses will appear in Spam:

You currently have no blocked addresses.

From \_\_\_\_\_

To \_\_\_\_\_

Subject \_\_\_\_\_

Has the words \_\_\_\_\_

Doesn't have \_\_\_\_\_

Size greater than \_\_\_\_\_ MB

Has attachment  Don't include chats

Create filter

Search

Create a filter using the domain name to block all email addresses from that location.

Ex: Filtering “gailborden.info” will block all emails from the library and staff.

# Purchasing Online



# Purchasing Online

- Use an electronic payment system for higher security. It is safer to keep your credit card information in one place.



**PayP  
al**



**Apple  
Pay**



**Google  
Wallet**



# Safe Internet Use

The image shows a screenshot of the SCAMADVISER.COM website. At the top left is the logo, a red shield with a white checkmark, followed by the text "SCAMADVISER.COM". Below the logo is a navigation bar with several tabs: "Check Website" (highlighted in orange), "Recent Checks", "Risk Sites", "About Us", "FAQ", "Forums", and "Trust Seal".

Below the navigation bar is a search input field containing "amazon.com" and an orange button labeled "Check it now". Below the search field is a large green banner with a white checkmark icon and the text "High Trust Rating. This Site Looks Safe To use."

Below the banner is a "Trust Rating" section. It features a "Click to See Reviews:" link and a "Comments" button. On the left is a small thumbnail of the Amazon.com homepage. To the right of the thumbnail are several statistics: "Popularity" with a "Very Popular" icon, "Last refreshed August 7, 2016, 6:41 pm", "Number times viewed :20242", and "Est Website Value :344142857.14". Below these statistics is a horizontal risk scale bar that transitions from red on the left to green on the right, with a green segment at the end. A dark grey box with a white checkmark and the text "Looks Safe (100%)" is positioned at the end of the scale bar.

At the bottom of the "Trust Rating" section, there is a text prompt: "Want to see what others are saying about them or even add your own".

# 2-Step Authentication

- Use credit cards with two step authentication for highest security
- Credit cards with 2 step authentication
  - Chase
  - Discover
  - Citibank
  - Bank of America
  - Charles Schwab
  - and many others

# Updating



# Updating

- Avoid using unsupported Operating system (Windows XP, Windows Vista, 7(2020), Mac OS X Leopard)
- Upgrade to the newest operating system for your device when possible
- Update your apps or programs when notified
- Set up automatic updates

# Privacy



# Turn off Google Tracking

1. Go to [myaccount.google.com](https://myaccount.google.com)
2. Click on **Data & Personalization**
3. Select the activity type to make changes

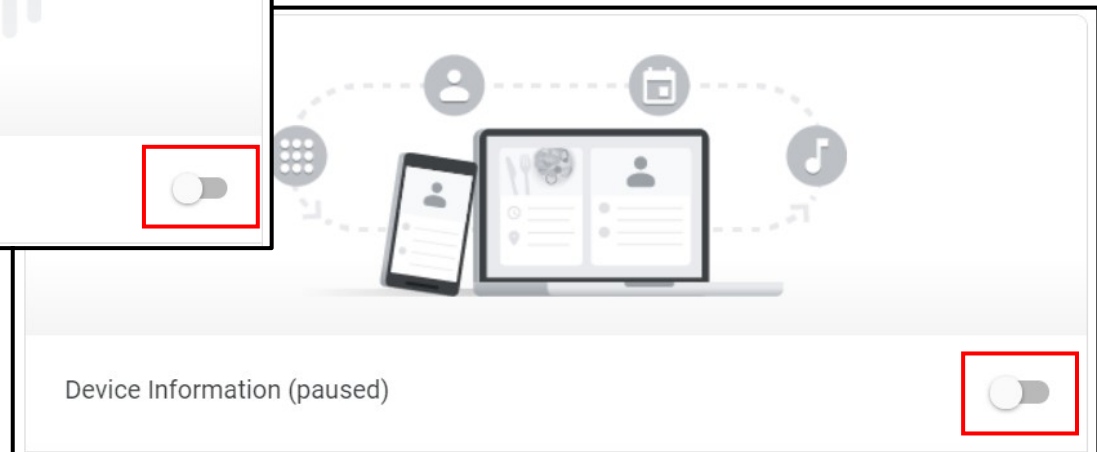
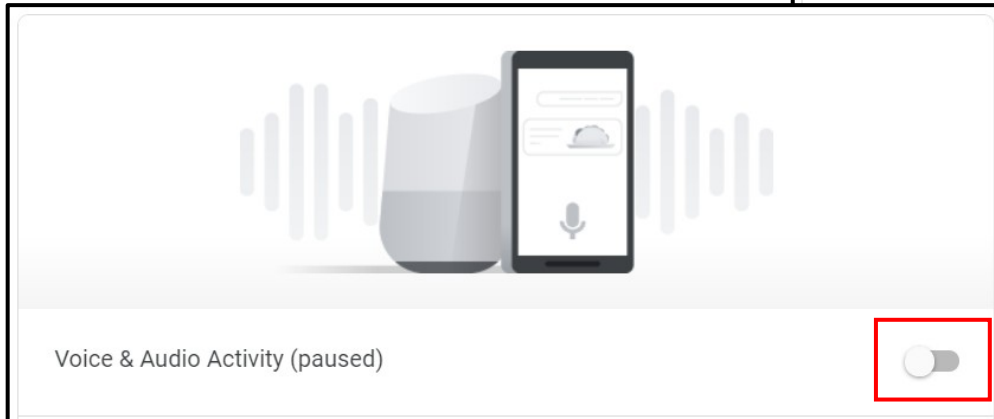
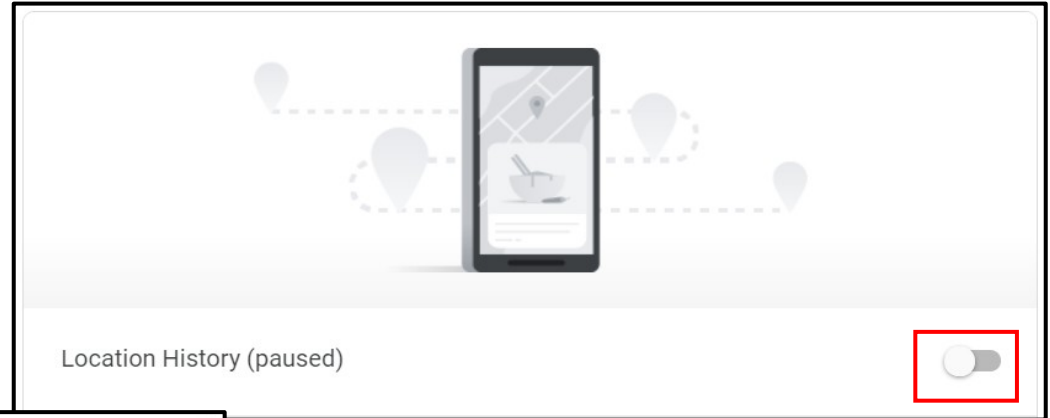
The screenshot shows the Google Account interface. On the left sidebar, the 'Data & Personalization' option is highlighted with a red box. The main content area is titled 'Activity controls' and includes a sub-header: 'You can choose to save your activity for better personalization across Google. Turn on or pause these settings at any time.' Below this, a list of activity types is shown with their current status:

| Activity Type          | Status |
|------------------------|--------|
| Web & App Activity     | On     |
| Location History       | Paused |
| Voice & Audio Activity | Paused |
| Device Information     | Paused |
| YouTube Search History | Paused |
| YouTube Watch History  | Paused |

At the bottom of the activity controls list, there is a link: [Manage your activity controls](#). In the top right corner of the page, the user's profile information is visible, including a blue circle with the letter 'D' and a 'Google Account' button, both highlighted with red boxes.

# Turn off Google Tracking

- Toggle off anything that makes you uncomfortable



# Privacy Emails



- End to End Encryption for truly anonymous email



- End to End Encryption for truly anonymous email



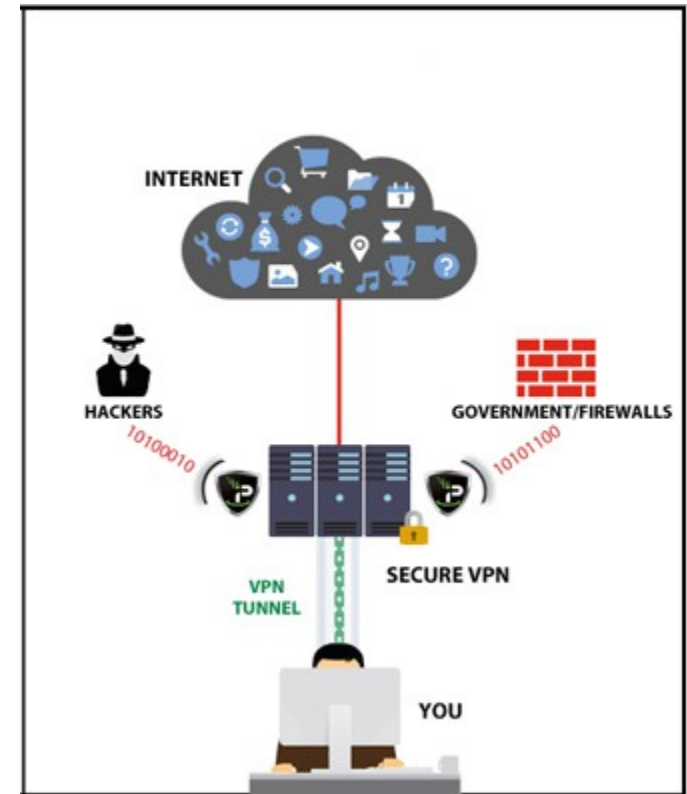
- Canadian provider that has been providing secure email since 1999



# Privacy VPNs

**For the best privacy use a  
VPN**

- What is a VPN?
  - Stands for Virtual Private Network
  - Encrypts your internet Data
  - Private web browsing, downloading, and uploading
  - Almost impossible to be tracked



# VPNs

## Free

- Opera developer browser has a free VPN built in
- Total VPN (Free)
- Cyber Ghost VPN (Free)

## Paid

- Total VPN paid version \$4.99 per month
- Private Internet Access VPN \$6.95 per month
- Nord VPN \$8 per month

# Private search engines

- DuckDuckgo.com



- Startpage.com

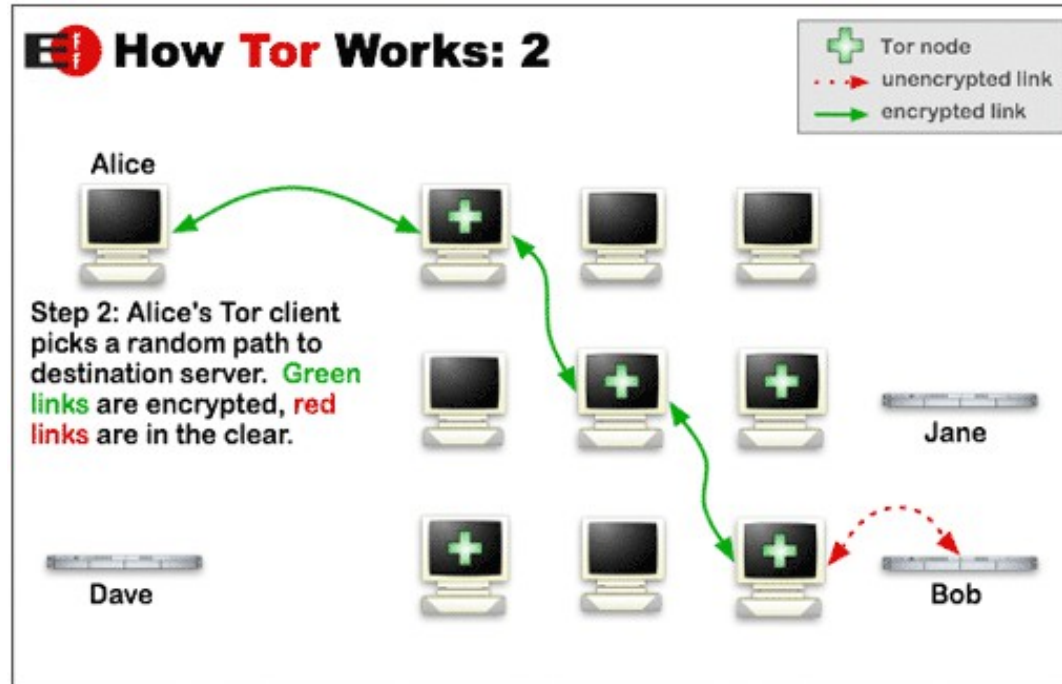


Uses Google search, but hides your information.

- These search engines **do not**...
  - Track your browsing info
  - Save your searches
  - Target you with ads
  - Use your past searches to bias the result

# Private Web Browser

- Tor browser
  - [www.torproject.org](http://www.torproject.org)
  - Prevents tracking
  - Creates an anonymous browsing experience



**Questions?**

**THANKS FOR COMING!**