Saved With A Click

Internet Security Basics

Presented by:

Ottawa Public Library

National Capital FreeNet

National Capital FreeNet | Libertel de la Capitale Nationale

Agenda

- Wi-Fi Fundamentals
- Wi-Fi Hotspots
- Public Computers
- Before Connecting
- Safe Browsing
- Top Safety Tips

Wi-Fi Fundamentals

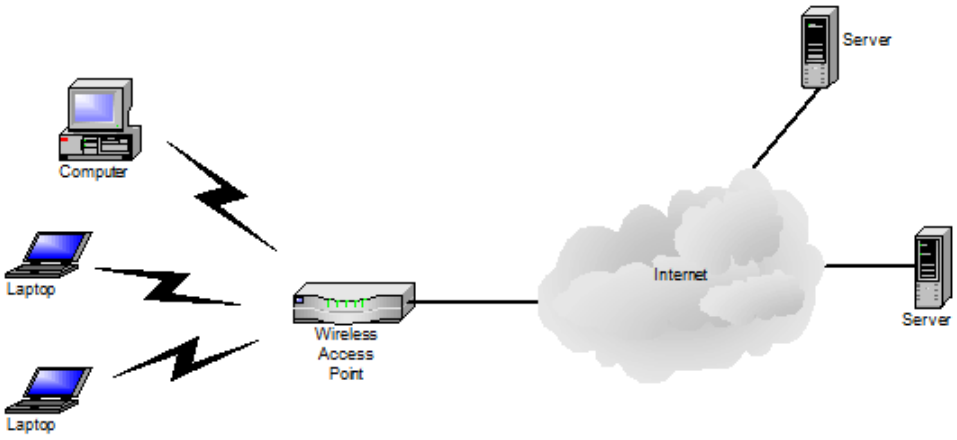
- Wi-Fi is a wireless network defined by IEEE 802.11
- Uses radio waves to provide two-way communication with an Access Point (Infrastructure mode) or another device (ad-hoc mode)

Wi-Fi Fundamentals (Con't)

- Transmits at varying speeds using frequencies of 2.4 GHz or 5 GHz
- Shared use of radio frequencies susceptible to eavesdropping
- Transmission security options include Open (none), WEP, WPA and WPA2

Wi-Fi Fundamentals (Con't)

- Access Point facilitates connection to the Internet



Wi-Fi Fundamentals (Con't)

- Access Point determines
  - Security type
  - Network (IP) address
  - Domain Name Server (DNS resolver)
- Even with transmission security (e.g. WPA2) Access Point sees all

Wi-Fi Hotspots

- Term used to define an area where Wi-Fi access is available, often free
- Typically have *Terms of Service* you must agree to before connecting your device to the Internet
  - Did you read it before agreeing?

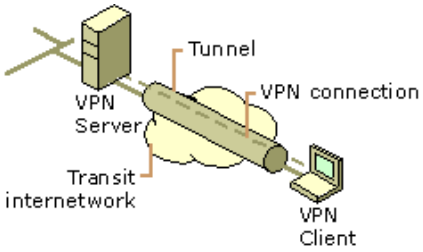
Wi-Fi Hotspots (Con't)

- Free Wi-Fi is convenient BUT can you trust it?
  - ***NO*** – network owner sees everything sent through the Access Point

- Don't risk your personal and financial information when using free Wi-Fi
  - Turning off Wi-Fi and using your cellular service is safer

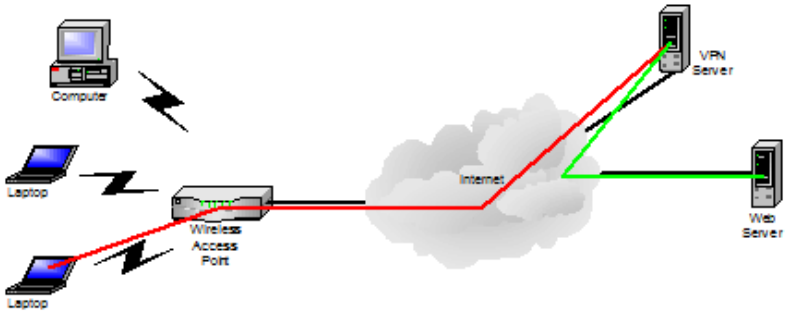
Wi-Fi Hotspots (Con't)

- Improved security available over free Wi-Fi by using a Virtual Private Network (VPN)
- VPN software on your device creates an encrypted tunnel to a server on the Internet



Wi-Fi Hotspots (Con't)

- Access Point or eavesdroppers only see encrypted data
- VPN service decrypts all traffic before sending it onward to the Internet



Wi-Fi Hotspots (Con't)

- Using a VPN shifts the confidentiality risk from the free Wi-Fi network to the VPN provider
- VPN providers usually charge for their services (see - https://www.privacytools.io/#vpn) but do provide confidentiality when using free Wi-Fi

Public Computers

- Internet Cafés offer computers with some form of online access for public use, usually for a fee
  - Ottawa Public Library offers free usage for library patrons
- Computers are configured by the provider and often restrict what you can do

Public Computers (Con't)

- Extra caution is needed because you don't know what software is running in the background
  - Key loggers?
  - Screen captures?
- Don't risk personal and financial data when using public computers

Public Computers (Con't)

- Safety precautions when using a public computer include:
  - Log out of any service you use
  - Clear the browser cache and cookies
  - Don't allow browsers to store passwords or other information
  - Delete temporary files

Before Connecting

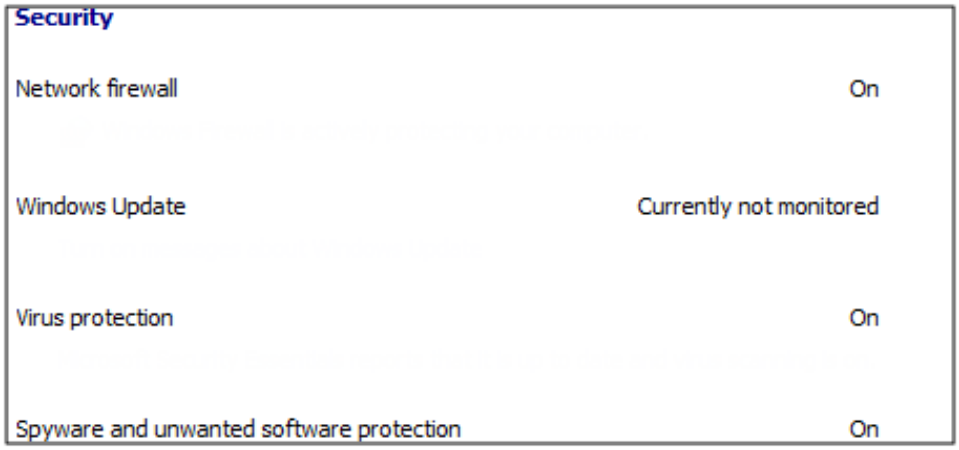
- Apply all security updates available from you device manufacturer
  - Computer OS has built-in update functions
  - Apple smartphones and tablets receive regular updates
  - Updates for Android smartphones and tablets are hit and miss

Before Connecting (Con't)

- Use an up-to-date and standards compliant web browser
- Don't use an unsupported OS and/or software
  - Vulnerabilities are well known and no longer being fixed

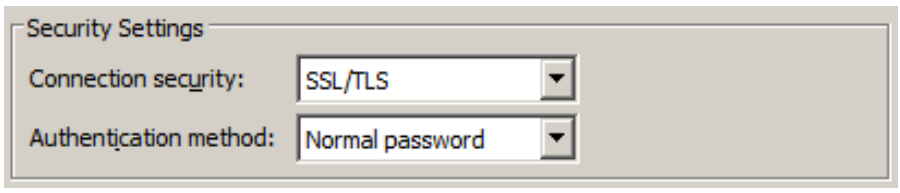
Before Connecting (Con't)

- Make sure your Firewall, Virus and Spyware protection are all turned ON



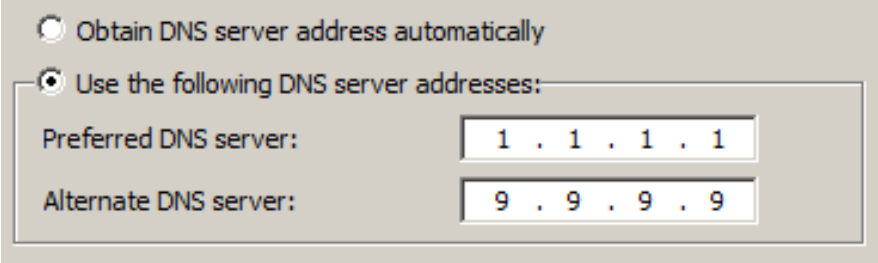
Before Connecting (Con't)

- Set your dedicated email program and/or app to use secure connections and passwords



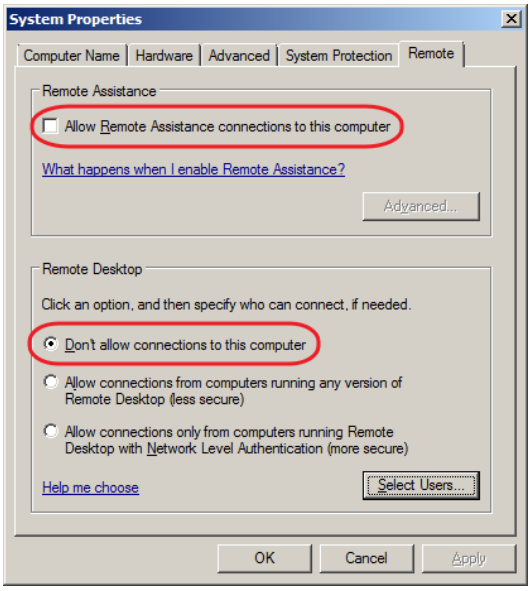
Before Connecting (Con't)

- Consider using a DNS service of your own choosing rather than the one the Access Point prefers



Before Connecting (Con't)

- Block remote access to your device

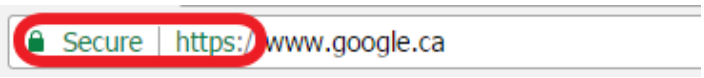


Before Connecting (Con't)

- Secure your on-line accounts
  - Use unique and complex passwords for each account
    - Password Managers make this easy and convenient (see - https://www.privacytools.io/#pw)
    - Don't let your browser store passwords
  - Use Two-Factor Authentication (2FA) when available

Safe Browsing

- Always use secure web connections so Access Point and other devices can't see the conversation
  - Check for HTTPS and a padlock icon in the address bar



Safe Browsing (Con't)

- Don't let your browser automatically enter information into forms
- Consider installing browser add-ons that:
  - force sites to use HTTPS where possible, e.g. HTTPS Everywhere
  - block ads, e.g. AdBlock Plus, uBlock Origin

Safe Browsing (Con't)

- Consider setting your browser to:
  - block pop up windows
  - ask permission to activate plug-ins
  - always show the full URL in the address bar
- Log out of sites when you are done

Safe Browsing (Con't)

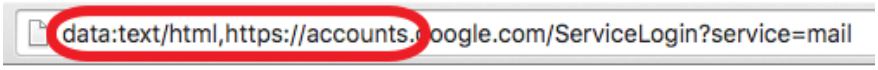
- When on a site where you need to enter sensitive information use only a single browser tab
- Question what you see
  - if a site pops up a window telling you that you need to install something for the site to work, DON'T DO IT – leave the site immediately

Safe Browsing (Con't)

- Use only reputable sites to:
  - download music, applications
  - stream music, movies and television
  - play online games
  - purchase things from online stores
- Verify the URL to ensure you are where you want to be

Safe Browsing (Con't)

- Make sure there is nothing before the HTTPS in the address bar

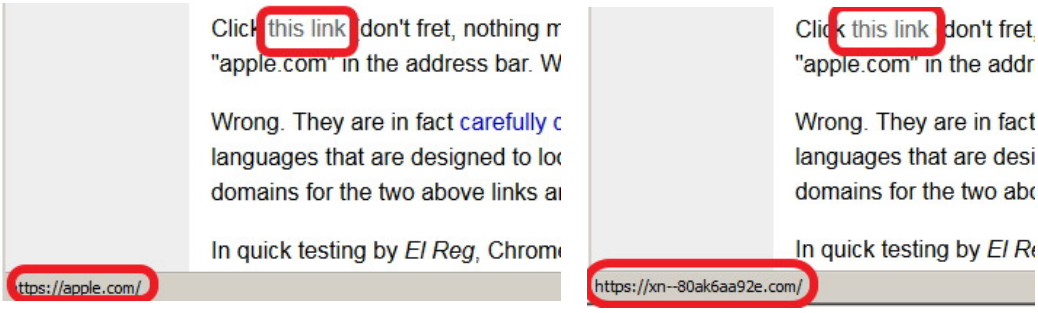


- Be wary of shortened URLs (e.g. bit.ly, goo.gl, etc.) – you don't know where they lead

Safe Browsing (Con't)

- Firefox currently vulnerable to a Homograph attack
  - Converts words that can't be written in ASCII (e.g. Cyrillic and Greek) into ASCII
  - Attack counts on the non-Roman fonts being absent

Safe Browsing (Con't)



- Force Firefox to display real value on the *about:config* page by setting the *network.IDN_show_punycode* property to true

Preference Name	Status	Type	Value
network.IDN_show_punycode	user set	boolean	true

Top Safety Tips

- Think before you click
- Get anti-virus protection and keep it updated
- Keep your computer software and apps updated
- Be careful on Wi-Fi Hotspots

Top Safety Tips (Con't)

- Create strong, unique passwords for every site
- Question what you see
- Download and stream from reputable sites only