Internet Concepts

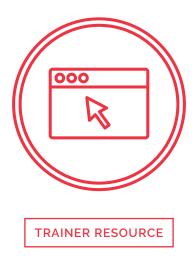TRAINER RESOURCE

This document is a reference and preparation sheet for the trainer, and a companion to the lesson plan.

The Learning Objectives summarize the knowledge that learners should have gained by the time they reach the end of the module.

The Background and Detail for Trainer provides greater details on the content, and links to references. It will allow trainers to learn more about the topic so they can lead discussions or answer questions confidently without being limited to the classroom content. Each item in the Background supports a section in the Lesson Script.

Learning objectives

> An understanding of the services available through the Internet

> An understanding of the technology underlying Internet security

> An understanding of the risks associated with different manners of connecting to the Internet

Background and Detail for Trainer

1   What the Internet is used for

1.1   In Brief

The Internet connects people and information through services such as email, games, social media, online banking, entertainment and video chat.

1.2   In Detail

- The Internet combines advances in information technology (which have greatly increased our capacity for storing and managing information) with advances in communications technology (which allow us to transfer greater amounts of information more easily).

- This means we can:

  - Access the kind of information we are accustomed to seeing in print and on television such as books, magazines news articles, shows, movies, etc.

  - Create and publish our own information.

  - Use new forms of media, like constantly-updated reference material and crowd-sourced publications such as:

      - Wikipedia.org;

      - Photo collections at the New York Public Library;[1]

      - Teaching initiatives such as Khan Academy;[2] and

      - Online research tools like Google n-Grams[3] and Wolfram alpha.[4]

- There are 3.2 billion Internet users, 2 billion of whom live in developing countries.[5]

- Besides the well-established uses such as email and online bulletin boards or forums, use of social media services is growing.

  - 62% of adults in the USA use Facebook; 70% of those use it daily.[6]

- Canadians generally use the Internet for entertainment, news, email (89%), banking (69%) and personal interests (64%). The popularity of video chatting and games is increasing rapidly.[7]

---

1   http://digitalcollections.nypl.org

2   khanacademy.org

3   https://books.google.com/ngrams

4   http://www.wolframalpha.com.

5   The International Telecommunications Union report on the state of the Internet is available at: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf

6   To read more on this survey see: http://www.pewinternet.org/2015/08/19/the-demographics-of-social-media-users/

7   For more information on how Canadians use the Internet see: https://cira.ca/factbook/2014/the-canadian-internet.html

serene risc

1.3 In Practice

DO use the Internet to enrich your life by gaining better access to information and as an additional way to communicate.

2   There are risks on the Internet

2.1 In Brief

The risks on the Internet relate mainly to:

- The difficulty of keeping information private on a technology designed for sharing;

- Knowing whom or what to trust; and

- Proving you are who you say you are.

2.2 In Detail

- The large-scale digitization and connection of information has a downside.

    – The information and technologies can be used for criminal purposes.

    – Criminals can take advantage of the current issues in authenticating identity and authorizing activities as well as of low-cost global access and industrial-scale automation to find new scams and frauds.

- The cost of cybercrime and cyber security is estimated in millions and billions of dollars.[8] However, estimations don't explain the privacy and security implications of the technology, and don't put the risks into a helpful perspective.

    – The situation as described and explained in countless studies on the subject point to a bad situation that is getting worse.

    – On the bright side, many of these studies point to education as a positive influence, so teaching this course is a step in the right direction.

2.3 In Practice

DO be aware of dangers online and learn to minimize risk.

3   The Internet is made up of connected computers

3.1 In Brief

- The Internet is made up of millions of computers linked together to allow information to flow freely between them.

---

8   100 billion per year (2013 US alone) — http://www.wsj.com/articles/SB10001424127887324328904578621880966242990

160 Billion per year (2014) — http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf

7.6 million per business (2015) — http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/index.html?jumpid=va_fwvpqe387s

- The technology used is very trusting. Security is not built into the Internet and should never be assumed.

3.2 In Detail

- The Internet developed out of many projects but a defining point in its establishment was the connection of a number of stand-alone research and university networks to enable greater communication.

  – The continuing development of the Internet reflects this, with a number of backbones connecting networks together for operation.[9]

- The technologies that enable the Internet are best understood as layers of operating protocols and common standards that work together to manage tasks as simple as passing a signal from one device to another or as complex as managing network services for applications.[10]

- You don't have to understand how everything works to use the Internet.

- To better understand security perspective it is helpful to understand how the Transmission Control Protocol (TCP)[11] and the Internet Protocol (IP) function.

  – TCP breaks messages down into tiny pieces, like tearing all the pages out of a book.

  – IP gets those pieces to the receiver, handling them like putting each page into a separate envelope (packet) and writing the address for the receiver and the sender on it correctly.

  – TCP puts them all the pages back together in the correct order for the receiver.[12]

- Routing is like a postal system. If you imagine a global system handled by a few billion volunteers, you understand the amount of trust in the handlers required.

  – Unlike a real envelope, TCP does not seal the package or show if it has been tampered with in transit.

  – There is no sure way to confirm that the envelope actually came from the sender and not from someone else.

  – Every one of the hundreds of systems that handle the message en route are trusted to not read, delete or alter the packages — ***but there is no way of knowing if they do.***

    ○ Because of this, it is important to keep information private by encrypting messages in packets in order to:

---

9   For more reading on the history of the Internet see: http://www.computerhistory.org/internethistory/

   http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet-related-networks

   http://www.livescience.com/20727-internet-history.html

10   There is a common way of thinking about these layers called the Open Systems Interconnect model. For a simple overview of the layers see: http://cisco.8bits.ca/osi/, and for greater depth see: https://support.microsoft.com/en-us/kb/103884

11   https://www.youtube.com/watch?v=7rR8p6gsExY

12   For greater depth on TCP/IP see: http://cs.smu.ca/~porter/csc/465/notes/net/internetprinciples.html

- Prevent others from reading them and

- Be sure that the contents are from the correct sender.

  ○ In an Internet browser, a web address starting with 'https://' indicates the use of encryption on the connection.

3.3 In Practice

DO check for security features such as encryption, before sending or receiving valuable information.

4   What is an ISP (Internet Service Provider)?

4.1 In Brief

An ISP provides a connection to the Internet. ISPs can provide service to a fixed point, like a home, or to a mobile point, like a cellular telephone.

4.2 In Detail

- Canada has many ISPs.

  – Many ISPs buy wholesale services from other ISPs and resell them.

- Access to physical infrastructure limits Internet access across Canada.

- How ISPs connect to the rest of the Internet is important to consider.

  – The far North of Canada is connected to the Internet via England, Ireland, Japan, Alaska and Seattle.

  – Much of the Internet traffic in Canada travels through the United States due to the major connection points to Asia near Seattle and to Europe in New York.[13]

  – Messages between two points in the same city, even the same house could travel to another country before reaching their destination.

- On a mobile device, you connect to your ISP through a wireless connection to a nearby service tower. The speed of mobile connections has improved over time.

  – Each advance was significant enough to be known as different generations of technology. We have advanced through 2nd Generation (2G) and 3rd Generation (3G). The current standard is 4G Long Term Evolution or 4G LTE.[14]

---

13 You can see some of the maps for this physical infrastructure at: http://business.shaw.ca/Wholesale/

http://arcticfibre.com/network/routing-map/

http://www.wholesale.bell.ca/our-network/

http://global-internet-map-2012.telegeography.com

14 http://www.3gpp.org/technologies/keywords-acronyms/98-lte

- The type of connection on your device is normally shown on the screen where the connection strength is shown (the bars). 3rd Generation and later connections offer good service and a level of security.[15]

- It is important to know who your ISP is as it is often a good source of support for issues that you might have connecting to the Internet.

4.3 In Practice

DO know how to contact your ISP.

Do look for a 3G, 4G or LTE symbol on your smartphone before using the Internet to ensure a safer connection.

5 The Internet at home

5.1 In Brief

- Broadband Internet connections allow home networks to access the Internet.

- Wireless home networks (Wi-Fi) should be used with the security features turned on.

5.2 In Detail

- A home Internet connection in Canada can connect through ADSL, DSL, fibre optic cable, coaxial cable and fixed wireless.

  - This connection is generally a broadband or high-speed connection,

    - These connections have similar properties; they are permanently connected and permit a high rate of data transfer.

  - Dial-up connections (an older type of connection that used the same wire as the telephone) have different properties. A dial up connection is considered technically inferior and should be unnecessary in Canada.[16]

- Internet at home starts with a cable connecting to a network in the street (or to an antenna in the case of fixed wireless).

  - This cable will be connected to a modem inside your home. A modem is a box with continually flashing lights that is generally supplied by your ISP.

  - A network router (wireless or wired) connects to the modem to manage communications to the Internet.[17]

---

15   2G networks and are vulnerable to eavesdropping. See https://media.blackhat.com/bh-dc-11/Perez-Pico/BlackHat_DC_2011_Perez-Pico_Mobile_Attacks-Slides.pdf for a technical explanation.

16   The CRTC has committed to providing broadband to all Canadians. http://www.crtc.gc.ca/eng/com100/2011/r110503.htm

17   Each ISP provides guides on installing a home network for each type of connection. They will normally send a technician to Install everything as some specialized knowledge and tools are required. An example of set up guides are found at: http://support.bell.ca/Internet/Connection-help/How-to-set-up-my-Connection-Hub#displayStep and http://support.videotron.com/residential/internet/installing-videotron-router/videotron-new-generation-wi-fi-router

- – The router and the modem maybe integrated into a single device.

- – All the Internet-enabled devices in your home connect to the router.

- Home Internet-enabled devices can connect directly to the router through wires or through the air over radio waves.

  - – Connecting with a wire keeps all the communications within the wire and provides a nice, controlled pathway for the signals but is a little impractical because the device is essentially tied to the wall.

  - – Wireless connections in a home network are possible with Wi-Fi technology.

    - ○ Wi-Fi technologies transmit data through the air and allow devices to move while transmitting and receiving data.

    - ○ They enable a single Wi-Fi base station to support a network with many devices.

    - ○ Neighbours have their own separate Wi-Fi networks even if they are within range of each other.

      - – This function relies on the devices deliberately ignoring messages that are not intended for them. This means that it is possible to listen passively just by not ignoring the messages.[18]

    - ○ Secure Wi-Fi requires a password to connect to the network.

      - – Devices without the password are unable to decipher the communications on the network.

      - – A secure network may be set up by default by the technician from the ISP.

      - – On an Apple computer a secure network is indicated by a padlock symbol next to the signal strength meter where the Wi-Fi network status is shown (usually by clicking on the Wi-Fi icon at the right of the menu bar, near the clock).

      - – On a Windows computer a secure network is indicated by the absence of a yellow shield next to the signal strength meter where the Wi-Fi network status is shown (usually by clicking on the Wi-Fi icon at the bottom right of the status bar, near the clock).

      - – WPA and WPA2 are security protocols used to encrypt all your information as it travels through your wireless network. They are more recent and offer more secure Wi-Fi networks than older protocols (WEP).

5.3 In Practice

DO ensure your home Wi-Fi network is secured with WPA or WP2 as the secure type and a unique and strong password.

---

18 For more detailed information on Wi-Fi see: http://pages.cpsc.ucalgary.ca/~carey/CPSC641/slides/wireless/WirelessTutorial.pdf

serene
risc

6 The Internet outside the home

6.1 In Brief

Networks outside the home can be less secure than a home network because more people use them.

Take extra care when sharing information if you connect to these networks.

6.2 In Detail

- A private network is one to which access is restricted to a known group of people or devices.

  - With a home network, you only give the password to trusted family members and friends who visit regularly.

  - With a corporate network, a company provides access to its network to a restricted set of people and maintains a list of their names.

- A public network has little restriction or accounting of who uses the network.

  - A local café where all customers get the password or it is written on a board is an example.

    - There is no way of knowing who or what is also connected to this network or what their intentions are.

  - This also applies to computers provided for public use.

    - There is no way of being sure that another user hasn't tampered with the computer before you started using it.

      - They might have installed software or devices that track your use and try to record your personal information.[19]

  - These systems may not be secure, as public networks make a valuable target to criminals due to the large number of network users who are potential victims.

    - Another issue with connecting to public networks is that you must trust the security awareness of the person providing the connection. Even major hotels have been affected with security issues that put the users of the private hotel network at risk.[20]

      - Be sure that you are connecting to the network provided by the hotel, not another unofficial network with a similar name. Connecting to an unofficial network would allow unknown administrators to be aware of your online activities.

---

19 To read about such a case, see: https://nakedsecurity.sophos.com/2011/02/14/hardware-keyloggers-discovered-public-libraries/

20 To read about this, see:

http://www.wired.com/2015/03/big-vulnerability-hotel-wi-fi-router-puts-guests-risk/

https://securelist.com/blog/research/71713/darkhotels-attacks-in-2015/

– Ask an employee for the exact name of their Wi-Fi network to make sure you are connecting to the correct one.

6.3 In Practice

DO be careful what information you share when connecting to public networks, wherever possible avoid sensitive transactions.

DO use your 3G or 4G connection if you have to send or receive private information outside the home.

Glossary of Terms

3G	The 3rd Generation Mobile telephone standard, capable of supporting telephony, internet access video calls and TV.
4G	The 4th Generation Mobile telephone standard, capable of supporting web access, gaming, HD TV, video conferencing and other services.
ADSL	Asynchronous Digital Subscriber Line is a set of technologies that allow for high-speed computer communications over a telephone wire at the same time as a telephone service.
Co-axial Cable	Co-axial Cable is a shielded communications cable that allows for the transfer of electric signals over a copper conductor.
Crowd-sourced	A system of making use of a large group of people to make decisions or perform work through solicited contributions rather than by using traditional employees or suppliers.
Digitization	The conversation of information to a digital form.
DSL	Digital Subscriber Line is a set of technologies that allow for high-speed computer communications over telephone wire.
Email	Electronic Mail.
Fibre Optic	Flexible, transparent glass or plastic cable that can transfer light from one end of the cable to the other.
Fixed Wireless	High speed wireless.

serene risc

Glossary of Terms (continued)

Internet Protocol	The protocol that regulates the transmission of data packets across the Internet.
Internet Service Provider	A company that provides access to the Internet as a service to subscribers.
LTE	Long Term Evolution is a protocol that allows for the provision of 4th generation mobile telephone services with greater efficiency.
Protocol	A set of rules and conventions for the transfer of information between devices.
Router	A device that manages the routing of information between computers and networks.
Social Media	A service designed to provide tools for socialising with others across the Internet.
Transmission Control Protocol	The protocol that regulates the formation and assemble of data packets for transfer across the Internet.
Video Chat	An Internet services that allows persons to chat while seeing each other with simultaneous bidirectional, real–time video feed.
Wi-Fi	A set of wireless computer networking technologies that allow for small networks.
Wi-Fi base station	A device that provides for a Wi-Fi network and often allows connection to a wired network.
Wireless	Sending and receiving electronic signals by using radio waves.
WPA, WPA2	Wi-Fi Protected Access and Wi-Fi Protected Access 2 are two security protocols designed to protect Wi-Fi networks. These protocols were developed to resolve issues in the earlier 'Wired Equivalent Privacy"(WEP) security protocol.

serene risc