Security 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 section.

Learning objectives

- New knowledge to overcome security myths and misconceptions
- An understanding of the value of information
- A security mind-set
- Awareness of malicious behaviour online

Background and Detail for Trainer

1 Being more secure, it's worth it

1.1 In Brief

Internet security can be managed by everyone, just by using good cyber hygiene, habits, and help.

1.2 In Detail

- There are some common excuses why people avoid putting effort into computer security, a discussion of these reasoning could be valuable.
- It's not my job
  - Security will always be partially your responsibility.
    - At home, you remember to lock your door. In public places, you remember to take your valuables with you.
    - Similarly, with your computer, you have to remember to not give away your passwords, and to check that your security protection is turned on.
- It's inconvenient
  - An ounce of prevention is worth a pound of cure.
    - Seatbelts in cars were also once considered to be inconvenient but they became a habit and they save lives.
    - Once you develop a few habits, they will become automatic and will save you a lot of trouble in the long term.
- It's too difficult
  - With a little education and a few good habits, it is easy enough for anyone to practise basic security.
    - Take your time and ask questions
  - Ensure that ***someone*** is taking care of security.
- I'm not at risk
  - Automation allows everyone to be a target of crime at the same time.
    - People are targeted indiscriminately.
    - It does not matter how much you have to lose. Even people with no money at all can have their identity stolen or their computer hijacked for a malicious purpose.

- I will get hacked anyway
  - It is possible to avoid many security problems but you will probably have to deal with some kind of security issue eventually.
  - Good habits and awareness can prevent a little issue from getting out of control and causing loss or harm.
  - You can minimize the chances of having a security issue, and reduce the impact of those issues from life changing to minor inconvenience.

1.3 In Practice

DO think of Internet security as something you can take responsibility for, by devoting a little time to it.

2 Your information and computer's resources are valuable

2.1 In Brief

Your information has value on the Internet: be careful how you give it away. Your Internet connection and computer's resources can be valuable to others.

2.2 In Detail

- Information is the currency of the Internet.
  - Your information and information about you are valuable to others.
  - Profit-seeking people and organizations are motivated to find out about you.
    - At times, they can overstep boundaries and invade your privacy.
    - At other times, the information you hold (such as credit card details) might be targeted by criminals.[1]
  - Be cautious when giving out your information.
    - This includes entering information into forms online and over the telephone.
    - Ask yourself if this website or caller needs this information.
    - If it seems suspicious, think twice about entering information or consider entering inaccurate (fake) information. There is no rule that you have to fill in every form accurately on the Internet.
    - If you are entering information on a webpage, consider leaving blank any boxes that are not mandatory (mandatory boxes are normally indicated with an '*').
    - If there you feel that a person or company's need to have your information is not genuine and justifiable there is no need to give it to them.

1 Example https://www.priv.gc.ca/cf-dc/incidents/2015/009_150710_e.asp

    - Criminals may try to take your information to pretend to be you and access your bank or take out lines of credit in your name.
  - Be careful when sharing information about yourself on social media.
    - Posting information such as your date of birth, address, family members and pets' names may give criminals information they can use to commit crimes.
    - This information can give them clues for your or your friends' or families' passwords, or provide information about what you have in your home and when you will be away.
- Your computer's resources, memory, ability to calculate and connection to the Internet can be of value to criminals.
  - You may think your computer contains no valuable information. Criminals disagree. You need to be vigilant about security.
  - The computer itself may be the objective of criminals. They may use your computer to attack other computers or to hide their identity.

2.3 In Practice

DO be careful when giving out your information online.

Do take action to protect your computer.

3 A security mind-set

3.1 In Brief

Thinking about security from a criminal's perspective can give you valuable insight for making decisions about your risk and safety.

3.2 In Detail

- Security professionals often refer to something called the Security Mind-set.
  - This is thinking about how security can be made to fail. Rather than thinking about ease of use, they think of ease of misuse. They do this to find problems that criminals can manipulate. Thinking like this can be helpful to find sources of risk for yourself. For example:
    - Convenience Mind-set > How easy is this password to remember?
      - Security Mind-set -> How easy is this password to guess?
    - Convenience Mind-set > How easy is it to open my account?
      - Security Mind-set -> How easy is it for someone else to open my account?
    - Convenience Mind-set > What is the minimum I have to know to access my bank?
      - Security Mind-set -> What is the minimum someone else has to know to access my bank?

- Thinking this way can help you to better understand the risk of a particular action, and act accordingly.
    - For example, if you are setting up an account that doesn't contain any personal information, you might not bother with maximum security because someone accessing it cannot do much damage.
    - The effect of somebody accessing your bank account would be much greater, so you make it difficult to do.
- Safety is a balance between convenience and security.
    - Sometimes the easiest option is best (low risk).
    - Sometimes the difficult option is best (high risk).
    - It is not possible or realistic to take the most secure option at all times, it is important to make a conscious and informed choice about how much security is appropriate for you.

3.3 In Practice

DO think about security before taking the easy option.

4 Online risks

4.1 In Brief

Criminals on the Internet try to trick people out of their money, their personal information or use software created with malicious intentions (malware), to automate the process. Security services (anti-malware and firewalls), encryption and a critical mind help defend against this.

4.2 In Detail

- Crimes on the Internet can be thought of as either targeting a person (tricking them or harming them directly) or targeting a computer (stealing resources or information).
    - Targeting a person:
        - Criminals can use the Internet's communications and the ability to publish independently to hurt, defraud and steal.
            - Criminals can contact more people from all around the world without meeting face-to-face, which makes the deception easier.
        - Be skeptical when dealing on the Internet since computers make it easy to forge documents, pictures and identities.
        - Be careful even when just talking about yourself or providing information. Criminals can use the information you share to steal your identity.
        - Phishing: Tricking you into giving information away is referred to as phishing.
            - You could be tricked into visiting a phoneyphony website that looks the same as a website you trust (like a bank's website).

- Against a computer:
    - Criminals can steal (copy without right or permission) personal information and data from your computer or when dealing with others on the Internet. They could manipulate the data or change them to deceive you.
    - Information can be stolen when it is stored on a computer or when it travels across the Internet between computers.
    - A great deal of this manipulation and stealing is automated and performed by computer software that criminals have downloaded or written themselves called malware.
        - Malware can be designed to:
            - Retrieve information from your computer (for example, copy files, record web activity or what you type).
            - Manipulate information on your computer (such as lock the information on the computer and demand a ransom).
            - Manipulate information you send (such as send email on your behalf).
            - Manipulate information you receive (such as change the results of a search).
        - When your information goes onto the Internet, it passes through other computers. These computers may contain malware that copies or manipulates your information.
        - Some malware uses your computer to attack other computers or websites. Controlling many computers allows criminals to automate more processes and distance themselves from criminal activity.
            - Because these infected computers operate without their owner's direction, they are called Zombies.
            - A large number of computers under the control of one person is called a Botnet (as in as a Robot network).
    - Security software can help, but only help.
        - Security software packages can detect malware on your computer.
        - A firewall can help prevent malware from reaching your computer.
        - Encryption can help prevent malware from reading or manipulating your communications.
            - For example, in an Internet browser, a web address which includes an 's', after the http (https://) tells you the connection is encrypted.
    - The best defence against fraud is a skeptical mind and being informed. If you feel you are being tricked, stop and discuss the situation with someone you trust.

4.3 In Practice

DO be aware of criminals.

DO keep your security service up-to-date, and use encrypted services for sensitive communications.

5 Good habits

5.1 In Brief

With a little effort, you can greatly reduce your risk. If you do have problems, help is available.

5.2 In Detail

- In real life, you have many years of experience and lots of education about staying healthy and safe. Conversations about safety from disease and crime are quite common. We regularly assess our health and crime risks, and act accordingly.
  - For example, we consider appropriate vaccines before travelling overseas but not to go to a friend's house.
  - This doesn't guarantee we will be safe but it helps.
- Good computer hygiene is making sure that your computer is set up, patched, and that your security software is updated and functional before you go out onto the Internet.
  - Good habits:
    - Think before you click;
    - Look for indicators of security; and
    - Think critically when dealing online.
  - Support is available from friends or advisors such as your financial services provider, your security services provider, the government, and the police.

5.3 In Practice

DO think of security in terms of good hygiene, good habits and good help that reduce your risk.

Glossary of Terms

Botnet	A network of remotely controlled computers on the Internet.
Encryption	A process of converting information to a form unreadable to untrusted parties that still contains the original information and is able to be read by the intended recipient.
Firewall	A computer safety barrier between networks or a computer and the network.
Malware	Software designed primarily for a malicious purpose.
Security Mind-set	A way of thinking about computers that focuses on security defects.
Social Media	Internet technologies designed for socialising and sharing such as Facebook, and Twitter.
Zombie Computer	A computer that is infected with malware that allows it to be controlled remotely and is part of a botnet.