

Setting Security and Privacy



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

- > Understand what security software is
- > Understand why you should cover the camera on your computer
- > Ability to configure security and privacy settings on your devices



Background and Detail for Trainer

1 Configuring security and privacy

1.1 In Brief

Setting passwords, switching firewalls on and checking privacy settings are important steps in securing your computer.

1.2 In Detail

- Computer password.
 - Use the password lock to open your computer—even if you are the only one who uses the computer.
 - A password provides a basic level of accountability within the computer and can prevent somebody else from seeing or using your data if the computer is lost or stolen.
 - A good password is as complex, long, unique and memorable as it is practical, see the lesson on 'Identifying yourself' for more help on passwords.
 - To change your password on:
 - Apple: Go to **Apple menu** at the top left of screen, then **System Preferences > Users & groups > Click Change password.**
 - Windows: Go to **Control panel > user accounts and family safety > Change password.**
- Computer firewall (computer network safety barrier):
 - To enable the firewall on your computer¹ on:
 - Apple: Go to **Apple menu** at the top left of screen, then **System Preferences > Security and Privacy > Firewall.** Turn the firewall on (you may have to click on the padlock icon at the bottom left of this box and enter a username and password to do this).
 - Windows: In **Search**, type **Firewall**, and then select **Windows Firewall.** Select **Turn Windows Firewall On.**²
- Computer privacy settings:
 - Devices connected to the Internet often communicate with external services.
 - In some cases, this communication can be more than expected or required.

¹ Windows firewalls are explained at: <http://windows.microsoft.com/en-US/windows-8/Windows-Firewall-from-start-to-finish>

² <http://windows.microsoft.com/en-us/windows-10/turn-windows-firewall-on-or-off>



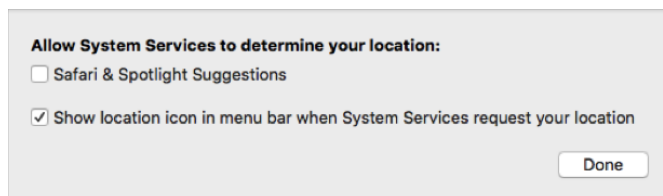
- o Make sure that the operating system is not sending out more information than you are comfortable with.
- o This is a balance and is a personal choice about what to share and which features are worth a loss in privacy. It is important to make a choice and not accept the manufacturers assumptions.

- Apple and Windows computers both have adjustable settings that control the amount of information sent out through the Internet.

- To choose to adjust settings for the greatest privacy, but lose some features:

- o Apple

- Go to Apple menu at the top left of screen, then **System Preferences > Spotlight > Search Results**, and uncheck the boxes for **Spotlight Suggestions** and **Bing Web Searches**.
- Go to **System Preferences > Security & Privacy** and select the **Privacy tab**.
- Select the **Location Services** tag.
- Select which applications can access to your location information.
 - If you don't want information to adjust automatically based on your location, turn them all off.
 - You can manually set your location for weather applications.
 - If you choose to have some applications access your location automatically, uncheck the other applications, click on the system services button and uncheck the **Safari** and **Spotlight Suggestions** option.



- Disable automatic web searches.
 - **System Preferences > Spotlight > Search Results** and uncheck the boxes for **Spotlight Suggestions** and **Bing Web Searches**.

- o Windows³


- Go to **Settings > Privacy > General**.
 - Let apps use my advertising ID: Turn this off.

³ For more information on the privacy settings for windows visit: <https://www.microsoft.com/security/online-privacy/overview.aspx>



- Turn on **SmartScreen Filter**: This is a feature to block some known malicious sites. Leave this on.
- Switch off Microsoft **how I write**.
- If you prefer French, websites providing local content can advise sites to switch language modes. Otherwise turn it off.
- **Turn Cortana Off.**
 - Bring up the **Start** menu and start typing. Click on the notebook icon in the left sidebar and choose **Settings**. Turn off Cortana.
 - **Search online and include web results**. When you turn off Cortana, this option will appear. Turn it off.
- Go to **Settings > Privacy > Speech, Inking, & Typing**.
 - Click the **"Stop Getting to Know Me"** button to **turn Getting to know you off**.
- Microsoft Edge (Windows 10's new browser)
 - Like most modern browsers (including Chrome and Firefox), Edge includes features that "phone home." You will find them in Edge's **Settings > Advanced Settings**. Here's what they do:
 - **Have Cortana assist me in Microsoft Edge** tracks your browsing history so it can reference it when you ask Cortana questions. You can turn this feature off in Edge's advanced settings.
 - **Show search suggestions as I type**. Edge logs your keystrokes to give you search predictions as you type. You can turn this feature off at **"Show search suggestions as I type"** here.
 - **Help protect me from malicious sites and downloads** with SmartScreen Filter. Leave this turned on.
 - Under **Settings > Privacy > Feedback & Diagnostics** are two settings:
 - **Feedback frequency**: change it to **Never**.
 - **Diagnostic and usage data**: Change this to **Basic**.
 - Location
 - Go to **Settings > Privacy Location**. If you plan to move a lot with the computer and would like it to update things such as weather settings automatically, leave them on here. Otherwise turn them all off.
- Mobile Device Screen lock
 - Locking the screen on a mobile device is very important. This provides a basic level of security. If the phone is lost, it makes it more difficult for someone to access your information and services.



- Where possible use a password with letters and numbers.
- Using the fingerprint scanning service is a good option. If you use a pattern, avoid simple shapes (L shape, triangle, square) and wipe the screen regularly to clean the smudge from the pattern from the screen. If you use a four-digit code avoid simple patterns (1234, 0000, 2580, 1111, 5555, 5683, 0852, 1212, or your birth year). These are not good passcodes.⁴
- iPhone
 - On devices with Touch ID (fingerprint scanner), Go to **Settings > Touch ID & Passcode** and **set a passcode**. Setting up Touch ID for iPhone unlock is handy too, just follow the prompts after selecting this option.
 - On devices without Touch ID, go to **Settings > Passcode**: Tap run pass code on.⁵
- Android
 - Open your device's **Settings** app . Scroll down and touch Security. Touch **Screen lock**.
 - If you already set a lock, enter the pattern, PIN or password before choosing a different lock.
 - Touch the screen lock you want to use and follow the instructions.⁶

1.3 In Practice

DO set passwords, turn on security and configure your privacy on your computer and mobile device.

2 Security software

2.1 In Brief

Security software helps manage your security. It is sold as a subscription that has to be renewed regularly. An anti-virus and active monitoring software package is recommended.

2.2 In Detail

- Security software is designed to protect you from malware.
 - Like locks on doors and bars on windows, they do not guarantee security.
 - No security software can provide total protection.

⁴ see <http://danielamitay.com/blog/2011/6/13/most-common-iphone-passcodes>

⁵ <https://support.apple.com/en-us/HT204060>

⁶ <https://support.google.com/nexus/answer/2819522?hl=en>



- It is not a substitute for caution. An airbag in a car will not prevent you from having an accident, and it won't help you if you are not wearing your seatbelt.
 - Its presence can prevent a little accident from becoming something far worse.
- It is very important to have security software to assist you, but it is only one part of your security plan.
- Electronics and office supplies retailers often have a large choice of security software.
 - There is no good way of recommending which product to buy, but there is a list of what not to buy. Many applications claim to be anti-virus software but are actually scams or viruses themselves.⁷
 - When buying security software, you are buying a service as much as you are buying a product.
 - Threats and malware on the Internet change constantly. Your security software should adapt to defend properly against them.
 - The company you buy your security software from will need to update it constantly.
 - Subscription details differ between offerings.
 - Ask how long the subscription is for and how many machines it protects.
 - Often, the subscription will need to be renewed each year.
 - Keep the subscription up-to-date to protect against current threats.
- Security software can affect your computer's performance.
 - This is because it reads files as you access them to make sure that they are safe.
 - There is no way to avoid this reduction in performance.
 - Software companies work very hard to minimize the impact of their software on performance.
 - Most of the popular security software providers (the kinds sold on those shelves) only reduce performance by a small amount.⁸
 - If your computer slows down a lot after installing new security software it may be for one or more of the following reasons:
 - The older software was not uninstalled;
 - There is not enough free space on your hard disk (approximately 20% is needed as a work area for the computer);

⁷ It is a big list and can be found at this site: <http://asafercomputer.co.uk/?q=Library>

⁸ For a performance comparison see: http://www.av-comparatives.org/wp-content/uploads/2015/11/avc_per_201510_en.pdf note that faster does not mean more effective.



- Software needs updating;
 - Too much software is running on the computer; or
 - The computer is just too old to run modern software (always read the system requirements before buying software).
- More is not better.
 - You should only have one security suite installed on your computer.
 - Having several running at once will result in conflicts that might slow down your computer or cause it to malfunction.
- Consider how intrusive the software is.
 - Some software will tell you constantly that it is working; others will work quietly in the background and nearly never let you know they are there. This is a matter of personal preference.
 - Most of the popular security software providers allow you to customize this element.
- Consider what functions come with the software.
 - This can be confusing, as there is a lot of marketing speak, jargon and flashy graphics. The functions of these software packages can be broken down into:

<i>What is it?</i>	<i>Also called</i>	<i>What it does</i>
Network security tools	Firewalls, intrusion detection systems, intrusion protection systems	Finds and stops bad network traffic (data in and out sent from Malware)
Active detection	Instant Messaging (IM) protection, anti-spam, anti-phishing detection, ad-blocking software, privacy filter	Finds software program code with malicious functions in the application you are using and blocks them
Content filter	Child filter, parental filter	Restricts the use of the computer to safer websites
Anti-virus	Anti-malware (virus, etc.), Windows Defender and Apple Security	Examines files as they are used and scans all files on a regular basis to determine if they are performing undesirable or unauthorized actions on the computer
Secure deletion	File Shredder	Deletes files so they cannot be recovered
Network and anonymity	Virtual Private Networks (VPN)	Provides a more secure connection and conceals your location



- Use a security service that provides anti-virus and active detection as a minimum security solution.
 - Computers with Windows 8 or newer and Apple computers come with some built-in protection.
 - These applications are not dedicated to providing security so they may not provide the same level of security or allow you to customize alerts and notifications as a specialized application.
- Be aware of service scams. Microsoft will not call you. A legitimate security software company will not call you.

Microsoft/Windows technician scam

Scammers call, pretend to represent a well-known company like Microsoft or Apple and claim that the victim's computer is sending out viruses or has been hacked and must be cleaned. The scammer will gain access to the computer remotely and may run some programs or change some settings. The scammer will then advise that a fee is required for the services and request a credit card number to cover the payment. In some cases, the scammer will send a transfer from the victims' computer through a money service like Western Union or MoneyGram. The result is that the victim pays for a service that was not needed as the computer was never infected.⁹

If you receive a call like this, do not provide any information to them. Hang up. You can report it to the Canadian Anti-Fraud Centre: 1-888-495-8501 or <http://www.antifraudcentre-centreantifraude.ca/reportincident-signalerincident/index-eng.htm>

2.3 In Practice

DO install security software to help you maintain the safety of your computer.

DO keep your subscription up to date.

3 Covering the webcam

3.1 In Brief

A webcam cover protects against spying through a webcam.

3.2 In Detail

- It is possible for an attacker to access your computer remotely without your knowledge.¹⁰
 - There are malicious programs that secretly provide another person with access to your computer; often called Remote Access Trojan programs (RAT).¹¹ A criminal might trick you into installing the malware by hiding it inside another file or program or by having you click a link or visiting a bad webpage. They can then see what you do on the computer, have access to your files and activate the camera and microphone.

⁹ See page 24 of the Canadian little black book of scams [http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/Little-Black-Book-Scams-e.pdf/\\$FILE/Little-Black-Book-Scams-e.pdf](http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/Little-Black-Book-Scams-e.pdf/$FILE/Little-Black-Book-Scams-e.pdf)

¹⁰ http://130.18.86.27/faculty/warkentin/SecurityPapers/Merrill/Thompson2005_CACM48_8_Spyware.pdf

¹¹ <http://www.trusteer.com/en/glossary/remote-access-trojan-rat>



- Covering the webcam ensures that they cannot see into your home and guarantees a minimum level of privacy.
- Covering your webcam is simple.
 - Just stick a piece of paper over the camera lens and only remove it when you are actually using the webcam.
 - You can also use the little sticky labels on bananas or other fruit and vegetables. They do not damage the screen and come off easily.
 - You can buy prettier webcam covers, but they do the same job as the piece of paper or the label.

3.3 In Practice

DO cover your webcam.

Glossary of Terms

Cortana	Windows personal assistant program that works with voice.
Firewall	A computer safety barrier between networks or a computer and the network.
Malware	Software designed primarily for a malicious purpose.
Scam	A dishonest or deceptive scheme usually for criminal purposes.
Scammer	A person conducting scams.
Screen lock	A barrier to accessing the function of a touch device by locking the screen.
Webcam	An Internet enabled (World Wide Web) video camera.