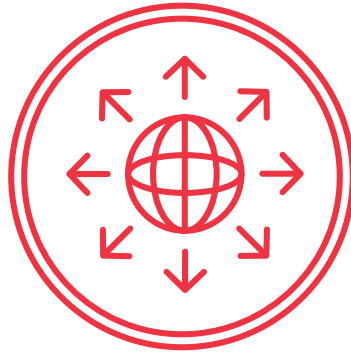


Going out onto the Internet



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

- > Understanding of the risks of browsing
- > Knowledge of what to look for in the browser
- > Ability to configure browser settings



Background and Detail for Trainer

1 The risks in the browser

1.1 In Brief

Advertising, tracking, drive-by downloads, man-in-the-middle attacks, typo-squatting and phishing all present different types of dangers to be wary of online.

1.2 In Detail

There are many forms of threat on the Internet. Being aware of common forms can help you to avoid some dangers and—more importantly—take action after encountering a threat to minimize the harm caused.

- Advertising
 - Intermediaries and large publishers (such as Facebook or Google), which we will call platforms, gather and analyze a considerable amount of data at very high speed, making it possible to customize advertising.
 - Advertisers can buy advertising in auctions with the cost depending on, the similarity of the webpage and the advertisement, your location, your browsing history, or information you gave to the platform or its partners such as through subscription questionnaires, or information posted on your social networking account posts.
 - These new opportunities give firms extra incentives to acquire and use personal information about consumers, which has led regulators and consumers to worry or at least to acknowledge some potential downsides of these practices.
 - Among the pitfalls are privacy breaches or fraudulent use of personal information, behavioural targeting and pricing.
 - As online advertising has become more popular, criminals have started to abuse it.
 - Malvertising is one of such activities, where an attacker uses advertising to distribute malware.
 - Malvertising can have serious consequences, because an attacker can place malware on popular websites. Therefore, the malicious content could reach a very large audience.
 - In addition, users may be unaware that they could encounter malicious content while browsing highly reputable websites, which may put them at risk.
- Tracking
 - Third-party online services bring tremendous value to the web: they enable websites to easily benefit from advertising, visitor counts, integrating with social networks and more.
 - They also give rise to privacy concerns.



- Third-party service providers make it possible for advertisers to track your online habits and browsing patterns across many websites, and tailor advertising to match these patterns.
 - o Personalized ads are considered to be the future of web advertising, and already make up a large portion of the global online ad market.
 - This increases the relevance of ads for users and their revenues for websites that have advertising on them.
 - This kind of advertising has raised concerns with respect to the use of third-parties to track and collect peoples' data.
 - People might not be aware of how they are being tracked between websites or the privacy implications and terms of service of the third-party service provider.
- Drive-by download attacks
 - A drive-by-download attack infects your computer just by visiting a page.
 - o Malicious programming in the page takes advantage of any vulnerability in your computer system, such as in the web browser or operating system to perform malicious actions or install other malware.
 - This can happen without you even noticing.
 - These pages could be controlled by criminals or they might undermine legitimate webpages.
 - 99% of webpages are okay.
- Typo-squatting
 - Typo-squatting is the deliberate registration of a domain name to exploit common typing errors made by users who type URLs into web browsers.
 - Simple and inexpensive domain registration motivates speculators to register domain names in bulk to profit from advertisements to redirect traffic to third-party pages, deploy phishing sites, or serve malware.
 - Very few website owners protect themselves by registering their own typo-squatting domains.
 - Typo-squatters target all websites, not just popular websites.
 - If the legitimate site is **example.com**:

<i>Typo-squatting address</i>	<i>Type</i>	
xample.com, example.com, xemple.com	Misspelled address	WARNING: Do not visit any of these sites. Some are known to contain malware.
example.org, example.biz, example.info, example.ca	Different domain (suffix)	
example.cm	Confusing domain suffix	



- Man-in-the-Middle (MITM) attack
 - In man-in-the-middle attacks, an attacker reads or alters Internet communications by inserting themselves between you and the intended receiver of your communication. Possible attacks and the impact of this kind of attack include:
 - Sniffing
 - Sniffing, or eavesdropping, is the act of reading traffic and collecting information.
 - Mostly, sniffing is used to steal credentials that are sent in plain text; without encryption.
 - Malware
 - Malware can be installed in many ways, such as redirecting you to a page or directly exploiting a vulnerability.
 - Binary patching
 - An attacker rewrites part of the code in the executable file to install malware or perform other malicious actions.
 - Cookie inserting/stealing
 - By stealing cookies, the attacker might be able to copy the user's session and thus log in as that user.
 - Cache poisoning
 - A cache is where a device can temporarily store some data to speed up future requests.
 - Cache poisoning happens when an attacker places forged data into the cache, which might lead to a browser connecting to the wrong IP address when visiting a site.
 - Fake certificates
 - Electronic certificates are used to verify the identity of a webpage. If attacker creates a fake certificate that is trusted by your computer, the attacker can pretend to be any site and listen in on encrypted connections.
 - Session hijacking
 - Some protocols work with sessions, which is like a formal conversation where the participants and time are defined. An attacker can hijack the session and pretend to be one of the participants.
 - Downgrade attacks
 - This is where the attacker interferes in the communication to restrict the use of newer (and safer) protocols or capabilities.



- Phishing
 - Your personal information can be very valuable to thieves.
 - In particular, usernames, passwords, bank and credit card details can benefit criminals.
 - Because of this, criminals put great effort into tricking people into giving away their valuable information.
 - Generally these efforts are referred to as phishing; as in phone fishing or fishing for personal information.
 - Phishing emails often appear to be from an organization with which you would have stored some valuable information.
 - These emails will often contain a link taking you to a page where you can log-in or enter valuable information on the pretext of checking something or updating something.
 - View links in email to pages asking for personal information or for your to sign into an account with extreme suspicion.
 - Avoid clicking on any link in an email from a bank (or Microsoft, Apple, PayPal...).
 - If you receive an email and want to check whether there is a real issue with your account, go to the website in the usual way or call the company.
 - Do not click on the email link, and do not copy the included URL into your browser.

1.3 In Practice

DO be aware of different types of threat so you can spot potential dangers to your information or your system.

2 What to look for

2.1 In Brief

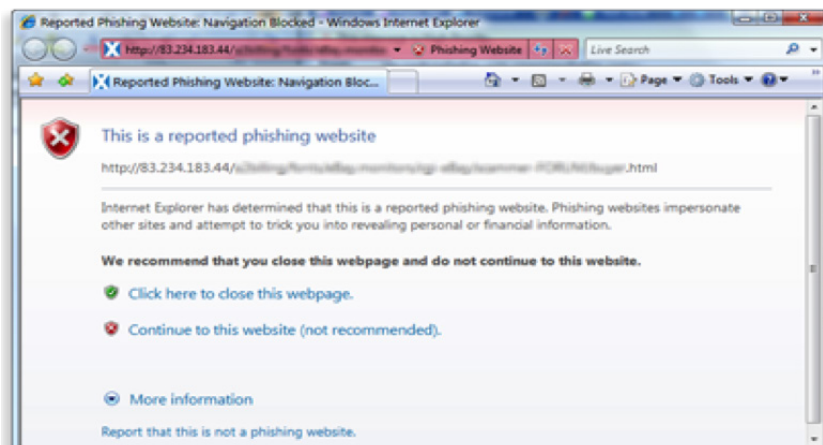
Browsers contain tools to help you navigate the web safely. Use them consciously in combination with critical thinking for a safer web experience.

2.2 In Detail

- When browsing, remember:
 - Trust the icons/cues that are part of the browser itself—NOT the ones within the content of the page.



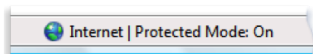
- A lock icon in the URL line plus “https” means that communication with the website is encrypted. It would be very difficult for anyone to eavesdrop on your data as it travels from your computer to the website. It does **not**, however, mean that the website itself is legitimate. Fake websites could also have a lock icon. Your data would be safe as they travel, but then would end up at a malicious website at the end point.
- A Green extended validation (EV) certificate box/green text means that the website has gone through some extra validation process to confirm that it is legitimate. It's not a guarantee, but it's a good cue.
- Combined, the lock and the green EV box give some assurance that you are visiting a legitimate site and that your data are secure as they travel to the site.
- All the content of a webpage can be faked.
 - Attackers can make exact copies of legitimate websites so that the fake ones look “professional.” They also make themselves look trustworthy by adding fake “seals.”
 - Do not rely only on the webpage content to determine legitimacy. Use the browser cues.
- Type in URLs yourself for known websites rather than trusting links.
- Look for the browser cues before entering personal or financial details like your credit card number or password.
 - If the browser warns you against visiting a page... take it seriously. Double-check the URL, make sure you have the right location.
- Identifying the security features of your browser
 - Internet Explorer
 - The phishing filter can help protect you from phishing attacks, online fraud and fake websites.



> Internet Explorer address bar with phishing warning

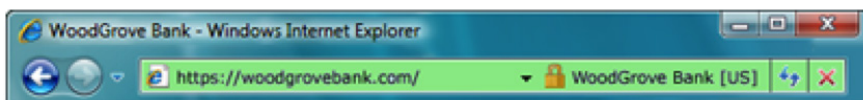


- Protected mode can help protect your computer from websites that try to install malicious software or to save files on your computer without your consent.



> *Protected Mode status indicator*

- Protected Mode status indicator
 - Higher security levels can help protect you from hackers and web attacks.
 - The security status bar displays the identity of secure websites to help you make informed decisions when using online banking or merchants. Internet Explorer now supports Extended Validation (EV) certificates to help make a more positive identification of website owners and organizations.



> *Security Status Bar (right side of address bar)*

- Internet Explorer security status bar (right side of address bar)
 - When you visit a website that uses a secure connection, the colour of the security status bar tells you whether the security certificate is valid or not. It displays the level of validation done by the certifying organization.
- The following table describes what the security status bar colours mean.

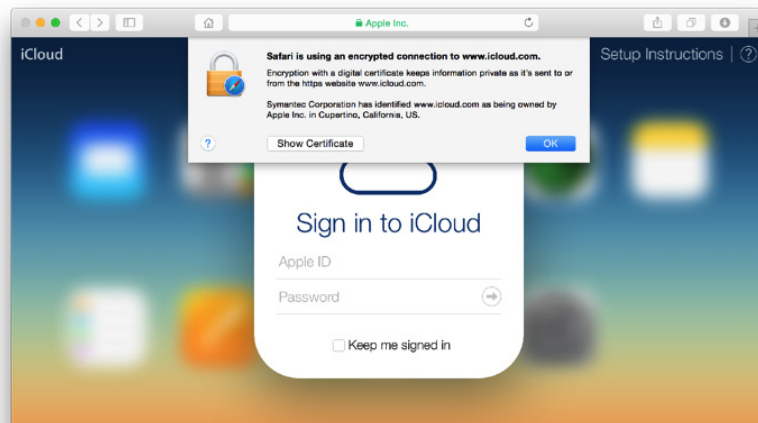
Colour	What it means
Red	The certificate is out-of-date, not valid or has an error.
Yellow	The authenticity of the certificate or certification authority that issued it cannot be verified. This might indicate a problem with the certification authority's website.
White	The certificate has normal validation. This means that communication between your browser and the website is encrypted. The certification authority makes no assertion about the business practices of the website.
Green	The certificate uses extended validation. This means that communication between your browser and website is encrypted, and that the certification authority has confirmed the website is owned or operated by a business that is legally organized under the jurisdiction shown in the certificate and on the security status bar. The certification authority makes no assertion about the business practices of the website. ^{1 2}

¹ <http://windows.microsoft.com/en-ca/windows/know-online-transaction-secure#1TC=windows-7>

² <http://windows.microsoft.com/lo-la/windows-vista/internet-explorer-at-a-glance>

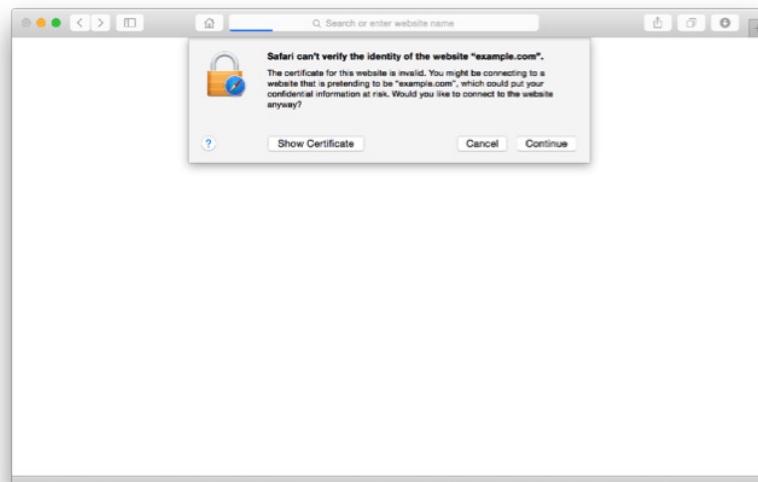


- Safari
 - o When you connect to a website with an encrypted connection in Safari, you will see a green lock icon in the toolbar next to the name of the company you have connected to (e.g.; Apple Inc.).
 - If you click the lock icon, you will see a dialog box saying that "Safari is using an encrypted connection to www.icloud.com." This tells you the connection is secure.



> *Connected to a legitimate site on Safari*

- o If you connect to a website that isn't secure, you will see a message that says "Safari can't verify the identity of the website." If you see this message, do not proceed or attempt to sign in.³



> *An unverified site on Safari*

³ <https://support.apple.com/en-us/HT203126>







– Chrome


- One of the most important security indicators in Google Chrome is where you enter web addresses; called the “omnibox” because it will take either a search or a webpage address.

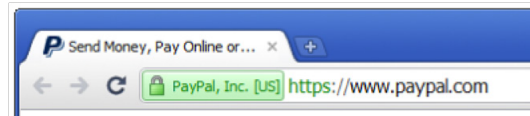


> *The 'omnibox' in Chrome*

- The first thing to notice is the domain name of the website. The domain name indicates which website is being displayed in the current tab. Google Chrome highlights it in a slightly darker colour. For example, the domain name in the image above is “www.google.com.”
 - Check that the omnibox has highlighted the domain name you expect. If the domain name doesn't match what you expect, the website might be fake.
- The second thing to notice is the lock icon, which is displayed to the left of the website address and, in the case above, coloured green.
 - This space will display the status of the connection and the page certificate. It can display any of the following:
 - Green lock icon 
 - The site's certificate is valid, and its identity has been verified by a trusted third-party. Google Chrome has established a secure connection with the site you're viewing.
 - Orange exclamation icon 
 - The site has not provided the browser with a certificate. This is normal for regular HTTP sites because certificates are usually provided only if the site uses encryption.
 - Webpage icon 
 - Your connection to the site is not encrypted. This is normal for regular http sites.
 - Lock icon with yellow warning triangle 
 - Google Chrome can see the site's certificate and your connection to the site is encrypted but the site uses a weak security setup or something unwanted on the page, so your connection might not be private.
 - These are common mistakes in website configurations.
 - Seeing this icon doesn't guarantee that your connection is secure. Proceed with caution and do not enter private or personal information on this page.



- Red lock icon 
 - There are problems with the site's certificate or mixed scripting.
 - Mixed scripting is when a page contains a mixture of encrypted and unencrypted content. It can be hard to know if using the page is safe or not. Proceed with caution.⁴
- Extended validation (EV) certificate (see green box over the lock icon and the web address in the image below).



> *An Extended validation Certificate from PayPal*

- The EV certificate helps the browser determine the name of the organization that runs the web site.
- The extended validation indicator helps you determine which organization is responsible for the displayed webpage. For example, the extended validation indicator for <https://www.benefitaccess.com/> says "Citigroup Inc. [US]."⁵

2.3 In Practice

DO look closely at the address bar to identify signs of security.

DO be careful to make sure you connect to the correct site.

3 Configuring the browser

3.1 In Brief

Dangerous websites are written with the same tools as legitimate websites, so it isn't possible to turn off just the unsafe tools. Learn what these tools are and how to make choices about what to allow in your browser.




3.2 In Detail

- Dangerous websites are written with the same programming tools as legitimate websites. They are an easy way to stay in touch with friends, family and acquaintances.
 - There are no bad tools, just bad programmers.
 - It isn't possible to turn off the dangerous tools without consequence.
 - Turning tools off can affect the operation of different websites in different ways

⁴ <https://support.google.com/chrome/answer/95617?hl=en>

⁵ <https://chrome.googleblog.com/2010/10/understanding-omnibox-for-better.html>





- Cookies
 - A webpage sometimes stores information in your browser; these pieces of information are called cookies.
 - This might be so that the page can remember who you are and your preferences. Often, it is to make a page more convenient for you.
 - Cookies allow the page to gather very precise information about how you use that page.
 - You can delete cookies. You can also block cookies using different levels of aggressiveness.
 - Blocking cookies can cause some websites to not function properly because they are designed assuming that you will allow cookies.
 - Sophisticated technologies allow companies to track your online activities without using cookies.
 - There is no easy and reliable manner to avoid tracking by these technologies. These methods mean that even if you block cookies you are not assured of privacy.
 - Be aware of cookies, and that they are not the only tracking technology.
- Blocking Cookies
 - Google Chrome
 - Select the Chrome menu icon. 
 - Select **Settings**.
 - Near the bottom of the page, select **Show advanced settings**.
 - In the "Privacy" section, select **Content settings**.
 - Select **Block sites from setting any data**.
 - Select **Done**.⁶
 - You can also remove cookies.⁷
 - Internet Explorer
 - Open Internet Explorer by clicking the **Start button**.  In the search box, type **Internet Explorer**, and then, in the list of results, click **Internet Explorer**.
 - Click the **Tools button**,  point to **Safety**, and then click **Delete browsing history**.
 - Select the Cookies check box, and then click Delete.⁸

⁶ <https://support.google.com/accounts/answer/61416?hl=en>

⁷ <https://support.google.com/chrome/answer/95647?hl=en>

⁸ <http://windows.microsoft.com/en-ca/windows7/how-to-manage-cookies-in-internet-explorer-9> and <http://windows.microsoft.com/en-ca/windows-vista/block-or-allow-cookies>



- Safari
 - o Choose **Safari > Preferences**, click **Privacy**, then do any of the following:
 - Change which cookies and website data are accepted. Select a “Cookies and website data” option:
 - Always block: Never store cookies.
 - Allow from current website only: Safari accepts cookies and website data only from the website you are currently visiting. Websites often have embedded content from other sources. Safari does not allow these third-parties to store or access cookies or other data.
 - Allow from websites I visit: Safari accepts cookies and website data only from websites you visit. Safari uses your existing cookies to determine whether you have visited a website before. Selecting this option helps prevent websites that have embedded content in other websites you browse from storing cookies and data on your Mac.
- IOS (iPhone, iPad)
 - o **Settings > Safari > Block Cookies** and choose one of the following:
 - o Always Block;
 - o Allow from Current Websites Only;
 - o Allow from Websites I Visit; or
 - o Always Allow.⁹
- Android
 - o Open the Chrome app: 
 - o Touch the menu; 
 - o Touch **Site settings**;
 - o Uncheck **Cookies** to prevent webpages from storing cookies on your mobile device.
- o JavaScript
 - JavaScript provides additional tools for developers writing webpages. It can also assist developers of malware.
 - Turning off JavaScript will make your browser more secure but it can also cause some webpages to not function properly

⁹ <https://support.apple.com/en-ca/HT201265>



- Turning off Java script is an extreme measure, and best only done temporarily if the risk associated with doing something is considered to be very high.
- Google Chrome
 - Select the Chrome menu icon. ☰
 - Select **Settings**.
 - Near the bottom of the page, select **Show advanced settings**.
 - In the "Privacy" section, select **Content settings**.
 - In the "JavaScript" Section Select **"Do not allow any site to run JavaScript."**
 - Select **Done**.
- Internet Explorer
 - On the web browser menu, click **Tools** or the Tools icon (which looks like a gear), and select **Internet Options**.
 - When the **"Internet Options"** window opens, select the **Security** tab.
 - On the **Security** tab, make sure the Internet zone is selected, and then click on the **Custom level button**.
 - In the Security Settings – Internet Zone dialog box, click **Disable for Active Scripting** in the Scripting section.
 - When the "Warning!" window opens and asks, "Are you sure you want to change the settings for this zone?" select **Yes**.
 - Click **OK** at the bottom of the Internet Options window to close the dialog box.¹⁰
- Apple Safari
 - While in Safari Click the **Safari Menu >Preferences**. In the Security panel uncheck the box marked **"Enable JavaScript."**
- Java
 - Java is not the same thing as JavaScript. Java helps translate Java programs for your computer.
 - This is helpful for programmers as they only have to write the program once without translating it for different types of computers.
 - It is also very helpful for people writing malware.
 - Java is not necessary for most of what you do with your computer, so it should be disabled.

¹⁰ For More and Site specific controls <https://support.microsoft.com/en-ca/kb/3135465>



- You may not have Java on your computer. However, if you do, turning it off will be a two-step process.
 - o Step 1 (Find the Java Settings Control)
 - Windows
 - Launch the **Windows Start** menu;
 - Click on **Programs**;
 - Find the **Java** program listing;
 - Click **Configure Java** to launch the Java Control Panel.
 - Windows (alternative method for older versions)
 - Use search to find the Control Panel;
 - Press **Windows logo key + W** to open the **Search charm** to search settings;
 - OR
 - Drag the Mouse pointer to the bottom-right corner of the screen, then click on the **Search** icon;
 - In the search box enter **Java Control Panel**;
 - Click on Java icon to open the Java Control Panel.
 - Mac OS
 - Click on Apple icon on upper left of screen;
 - Go to **System Preferences**;
 - Click on the Java icon to access the Java Control Panel.¹¹
 - o Step 2 (Turn off Java – the same for Windows and Mac OSs)
 - In the **Java Control Panel**, click on the **Security** tab;
 - Deselect the check box for **Enable Java content** in the browser. This will disable the Java plug-in in the browser;
 - Click **Apply**. When the Windows User Account Control (UAC) dialog appears, allow permissions to make the changes;
 - Click **OK** in the Java Plug-in confirmation window;
 - **Restart the browser** for changes to take effect.
 - o Privacy mode
 - Many browsers offer a privacy mode designed to offer some privacy to users who share computers.

¹¹ More detail and alternatives for Apple Safari: <https://support.apple.com/en-us/HT202447>



- The browser will not keep the history for the session.
 - This is not perfect privacy. You will not be anonymous while in this session.
 - The privacy offered by this mode is only local, and does little to mask your identity to the world.
- Opening a window in privacy mode is generally done by clicking the file menu and selecting a new private window.

This is called something different in each browser, and there are variations on how to open a window. The Shortcut keys to open a new window or tab are quite consistent. On windows press the 'Ctrl' Key, on an Apple Computer use the Command '⌘' key instead.

Browser	Privacy Mode Name	Shortcut Key
Safari	New Private Window	Ctrl (⌘) + Shift + N
Chrome	New Incognito Window	Ctrl (⌘) + Shift + N
Firefox	New Private Window	Ctrl (⌘) + Shift + P
Internet Explorer	InPrivate Browsing	Ctrl (⌘) + Shift + P

- Ad blockers
 - Ad blockers can be added to browsers to block the advertising content in pages.
 - This can help security because some advertising can be used to distribute malware.
 - These are third-party applications. We do not recommend any particular application but do recommend that you buy from official vendors.
 - Examples and information can be found at:
 - <https://getadblock.com>
 - <https://adblockplus.org> ¹²
- Flash
 - Flash allows interactive content. It was developed in the late 90s, and has been very popular because it has many powerful tools.
 - Newer, better tools have been developed.
 - Flash is used less and less. It has been abused to install malware.

¹² This is not an endorsement of either of these products. We have not tested them in any way.



- Chrome
 - **Type** `chrome://plugins/` into Google Chrome's location bar and press Enter. Click the **"Disable"** link under the Adobe Flash Player plug-in.
- Internet Explorer
 - Click the gear menu, and select **Manage add-ons**. Click the Show box and select **All add-ons**. Locate **Shockwave Flash Object** under **Microsoft Windows Third-Party Application Component**, select it, and click the **Disable button**.
- Microsoft Edge
 - **Click the menu button** in Edge and select **Settings**. Scroll down to the bottom of the Settings panel and click **"View advanced settings."** Set the "Use Adobe Flash Player" slider to **"Off."**
- Apple Safari
 - Click the **Safari Menu >Preferences**. In the Security panel, click **Security**. Then click the **Plug-in Settings button**. In the next panel, with Adobe Flash selected at the left, select **Block** from the menu at lower right of the screen (immediately above the Done button). Click **Done** and exit the settings menu.¹³

3.3 In Practice

DO disable Java and make an informed choice about Cookies, JavaScript, advertising blocking and Flash.

DO use the privacy mode to browse discreetly.

4 Putting it into practice

4.1 In Brief

Put what you have learned into practice. Remember to take care with the webpage address, look for security indicators, and warning messages when using an Internet browser.

4.2 In Detail

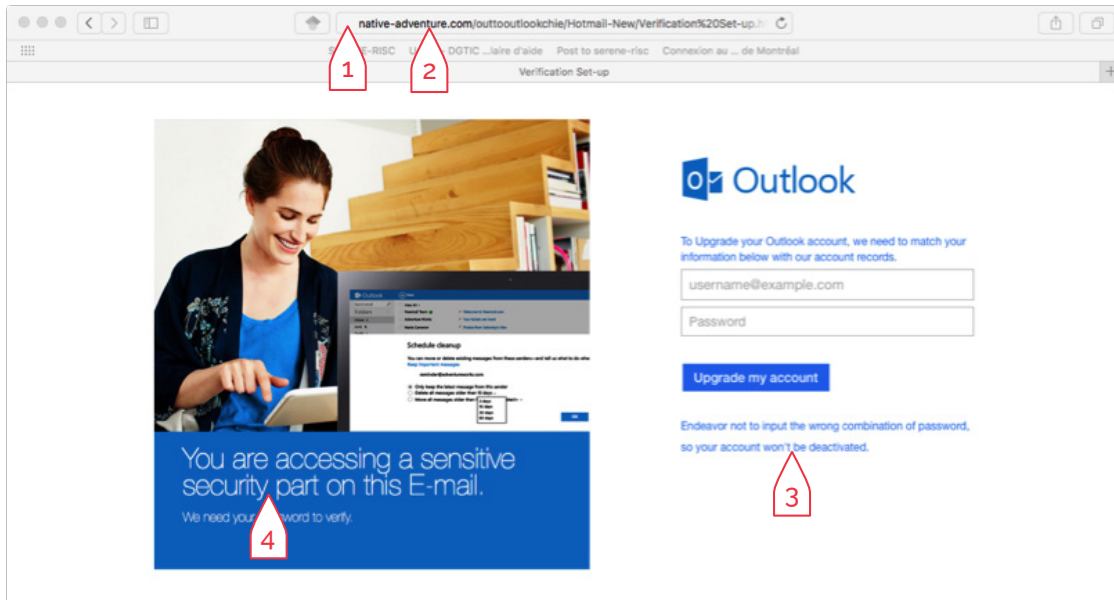
- The following is an example of navigating to a page and identifying a potentially dangerous website.
 - Typing in the URL
 - Go to **"outlook.com,"** type carefully and check before pressing **Enter**.
 - **BEWARE of "uotlook.com." It redirects to a potentially dangerous page.**
 - **Look for IP addresses** in the URL (numbers only) or addresses similar to the one you want but not quite.

¹³ <http://gizmodo.com/disable-flash-1688209571>

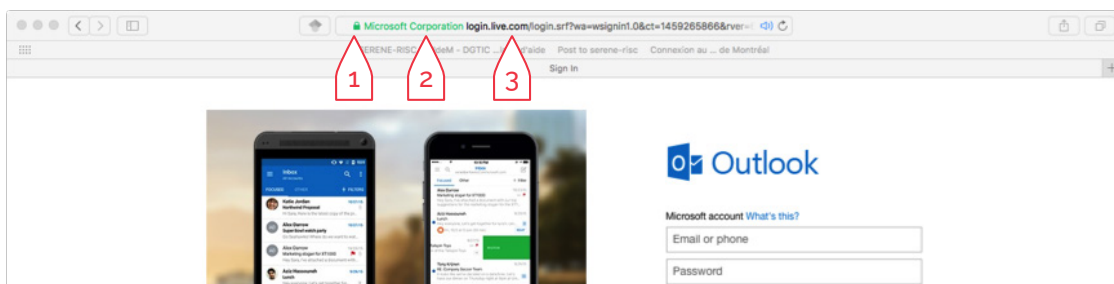


- Also **look for misspelled domain names** and subtle substitutions such as 0 for O or vv for w.

- Assessing the page

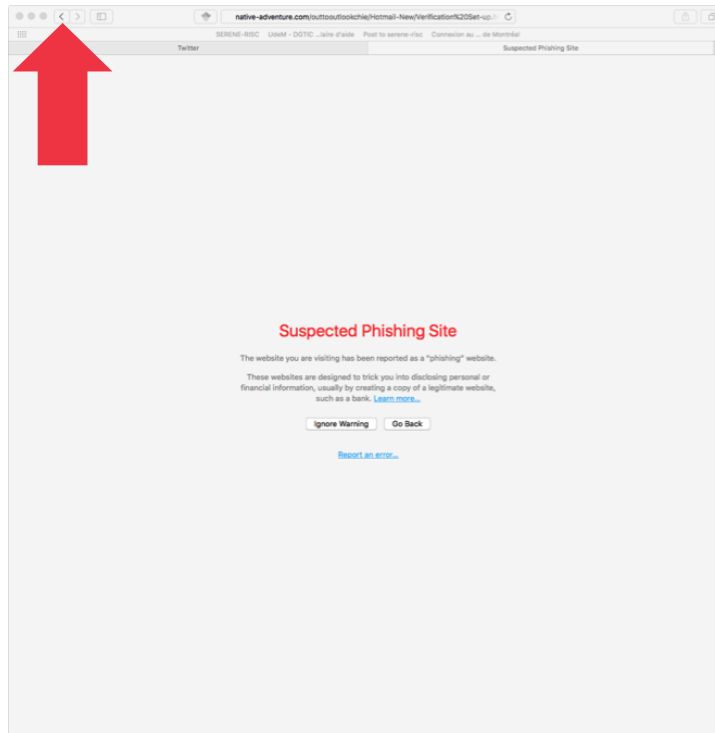


- o A number of clues on this page show that it is dangerous. Two are very clear indicators (1&2). Two are less clear (3&4) but add to the assessment.
 1. There is no lock icon or green in the address box. This tells us that the page is not using a secure connection and that there is no certificate. We expect that our outlook.com page would have both.
 2. The domain name is not a Microsoft name. "native-adventure.com" is not a name that we would expect to see. This indicates that this page is probably a fake used for phishing.
 3. Threatening language. It is not normal for a legitimate business to threaten their customers with account deactivation.
 4. Poor grammar. A major corporation like Microsoft is unlikely to publish a page with poor grammar.
- o Some indicators on this page provide clues that the page is legitimate:





1. A green lock symbol. This indicates a secure connection.
2. A certificate belonging to the organization you would expect to own this website.
3. The domain name is a bit odd. However, the green box showing ownership provides reassurance. (Live.com is a brand used to unify a number of Microsoft services to assist with living; such as Hotmail, outlook, and MSN Messenger).
 - o Also, note the lack of grammar errors or threatening language.



- o A page like this is a clear warning that the page is dangerous. This page is shown when the browser has identified the page as a problem. Press the Back button and avoid the website.
- o If you think you have made a mistake, change your passwords immediately.
 - If the account was for a bank, check your statements and contact your provider if there is an issue.
- o If you think you or someone you know has been a victim of fraud, please contact the Canadian Anti-Fraud Centre at:
 - 1-888-495-8501 or report online at <http://www.antifraudcentre.ca>.

4.3 In Practice

DO take care with the web address, look for security indicators and heed warning messages.



Glossary of Terms

Browser	A browser is a computer program or mobile app that is used to find and look at information on the Internet.
Cache	A cache is where a device can temporarily store some data to speed up future requests.
Certificate	Electronic certificates are used to verify the identity of a webpage
Cookie	A small piece of information stored on a persons browser for use by a website.
Domain name	The name given to help find a computer on the Internet (e.g. serene-risc.ca).
Drive-by download	A drive-by-download attack infects your computer with malware just by visiting a page.
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.
Extended validation certificate	A certificate that shows that website has gone through some extra validation process to confirm that it is legitimate and indicates the owner of the page.
IP address	An Internet Protocol (IP) address is a set of numbers that a device (computer, printer, etc.) on the Internet uses to identify itself (e.g. 206.167.212.121).
Malvertising	Malicious programs hidden in advertising.
Malware	Software designed primarily for a malicious purpose.
Man-in-the-middle attack	A malicious attack against communications executed between the sender and receiver.
Operating system	An operating system is the main program in a computer such as windows or Apple OSX that makes it possible for other programs to function.
Phishing	Emails, calls or other communication designed to trick you to give away personal information or passwords.