4 Tips for Safely Conducting Research on the Web

By S.E. Slack

Surprisingly, basic safety is often ignored by people using the web to research information quickly and efficiently. If you use the Internet for research of any kind, you could be exposing yourself and your company to hidden dangers such as the unauthorised transfer of confidential information. And no one wants to be the person responsible for a companywide computer network shutdown.

Whatever your reason for using the web, there is a smart way to conduct research on it: with an alert eye and a vigilant approach. Use these four tips to help protect yourself and your company from prying eyes and malicious programs.

1. Update, update, update!
Microsoft continually provides enhancements and security updates to all its products, including Internet Explorer. No program is completely safe from harm but as threats are discovered, Microsoft makes fixes, upgrades, and service packs for its products available. To maintain the highest level of security on your computer, you or your IT department must make sure to apply all service packs.

Before you venture onto the web, make sure you are using the latest version of Internet Explorer. At the time of this writing, the latest version is Internet Explorer 8.0.7. To see what version you are using, follow these steps:

1. In Internet Explorer, on the **Help menu**, click **About Internet Explorer**. There are three items you should notice in the window that is displayed:
   - **Version**: Internet Explorer (http://windows.microsoft.com/en-US/internet-explorer/products/ie/home) 8.0.7 is the latest version.
   - **Cipher Strength**: This is the level of encryption that the browser can support. If you are going to be sending any confidential information over the Internet, you must make sure the cipher strength is 128-bit. If it is less than this value, it will be possible for a hacker to crack the encryption code and view confidential information.
   - **Update Versions**: Keep your version updated to ensure the balance between security and functionality is correct.

Use latest version of Internet Explorer

2. Click **OK** to close the window.

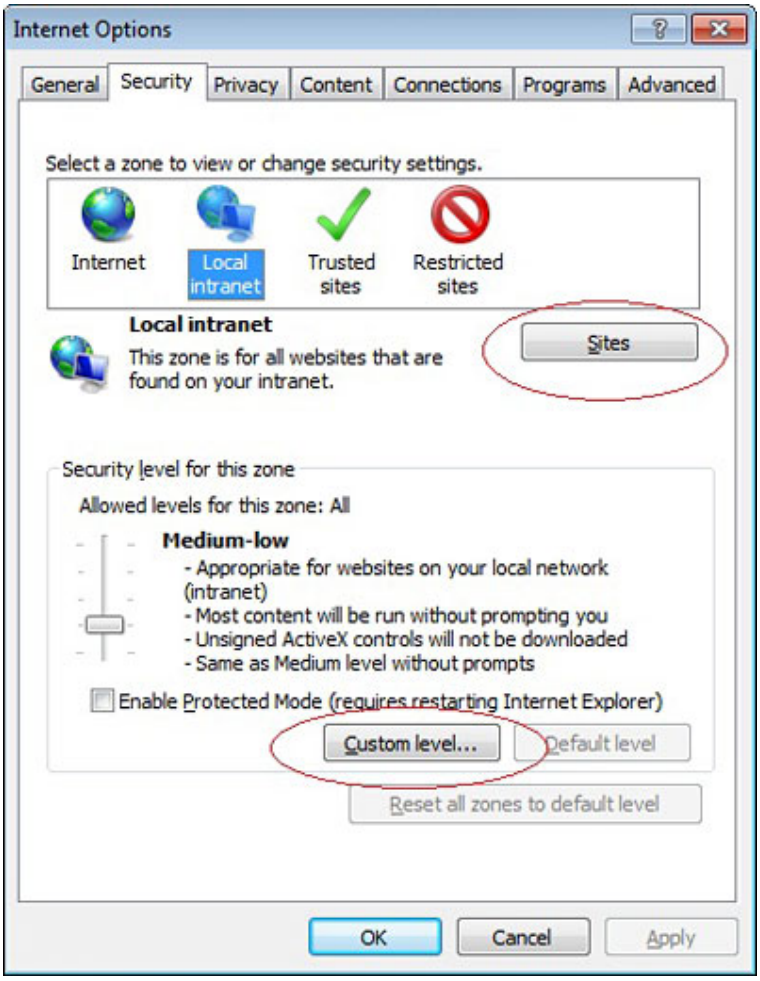
If your browser needs updating, go to the Microsoft Update (http://update.microsoft.com/microsoftupdate/v6/default.aspx?ln=en-us) website, where you can download the latest version of Internet Explorer.

2. Get into the zone

By setting up Internet zones to meet your personal needs, your computer can help protect you as you surf the web. A zone is a logical region or grouping of websites, based on where they are physically located and how well you trust the source. These default zones are available in Internet Explorer 8.0.7:

- **Local Intranet** – Websites located on your local network. These sites do not have to communicate over the Internet to be accessed.
- **Trusted Sites** – A list of websites that you trust not to harm your computer, such as sites you have identified as properly encrypted.
- **Restricted Sites** – A list of websites that are known or suspected to be harmful to your computer.
- **Internet** – All other sites that don't fall under the other three categories.

You can indicate how Internet Explorer should behave when it accesses a website within each of these zones. In Internet Explorer, on the **Tools** menu, click **Internet Options**. In the Internet Options dialogue box, click the **Security** tab.



Internet zones can help protect you

When you select a web content zone, you can change the security levels. For all but the Internet zone, you can add specific sites to a zone based on your personal requirements. And Custom Level allows you to enable or disable a variety of options based on personal preference. For example, you

may want to allow automatic logons only to websites that are located in your Intranet zone instead of everywhere on the Internet. The User Authentication section of the Custom Level zone allows you to set that preference. Or, you may want to ensure your Pop-up Blocker is enabled. Custom Level is where you can ensure your security settings allow your blocker to operate.

Follow the prompts in the Internet Options dialogue box in the zone you want to customise by either clicking **Sites** or **Custom Level**.

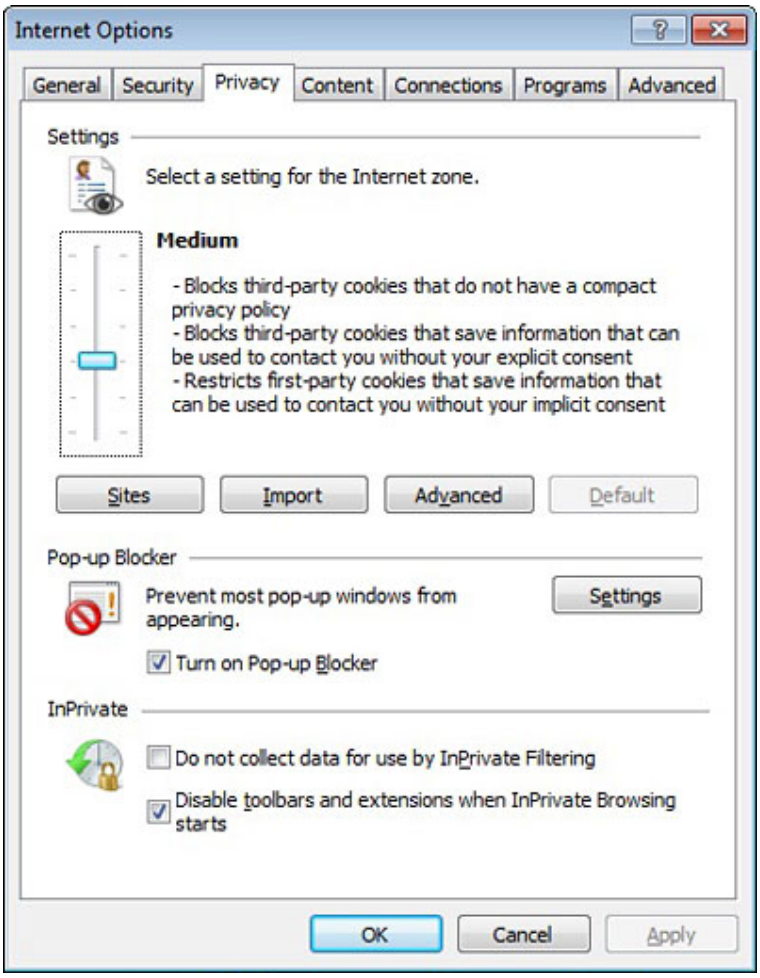
3. Limit your intake of cookies

Cookies are small files stored on your computer that contain information needed on certain websites. A cookie can be used to store user ID, password, preferences, personalisation, or other information that is helpful to enhance your experience on that site. For example, suppose you visit a website that allows you to select a preferred language. So you don't have to choose the language preference each time you enter the site, a text file on the site stores language preference directly on your computer as a file, or cookie.

Here's the catch: you don't know what the cookie has been programmed to collect. You don't know if the cookie is malicious or not. If it's malicious, you could quickly end up with a spiteful little program stored directly on your hard drive. A malicious cookie can collect and store almost any information that you may not want it to, such as your name, credit card information, address, or more. Cookies make it possible for unwanted information to be stored and accessed repeatedly when you visit a website.

By default in Internet Explorer, cookies are allowed for all zones except the **Restricted Sites** zone. However, if you want to limit cookies for a particular zone, here's how you do it:

1. In Internet Explorer, on the **Tools** menu, click **Internet Options**. In the **Internet Options** dialogue box, click the **Privacy** tab.
2. In the Settings section, move the slider up or down to adjust the settings.



Select settings for Internet Zones

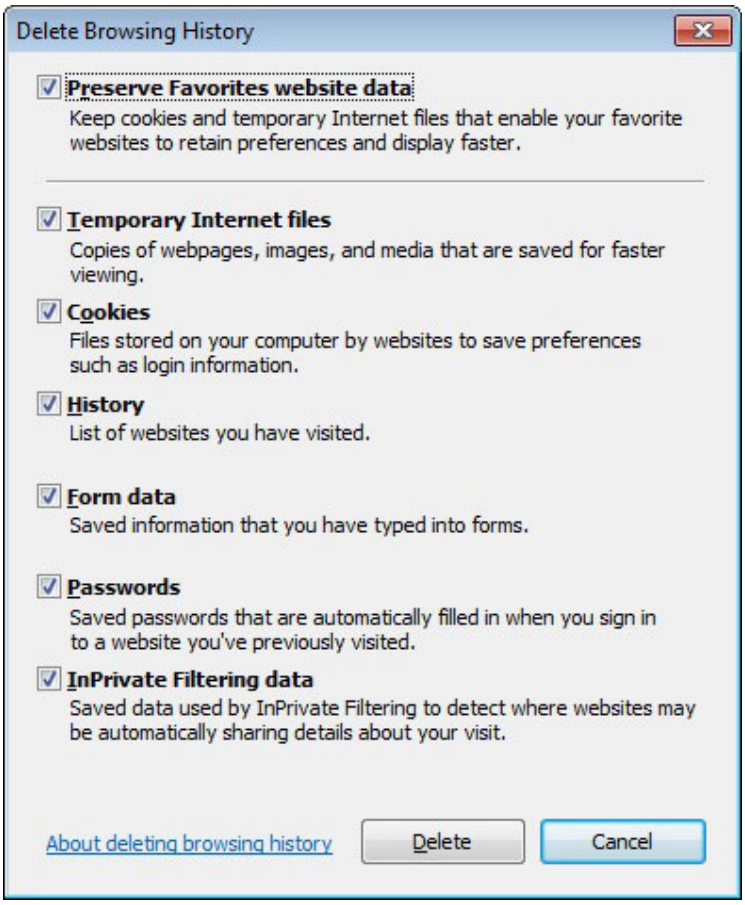
Moving the slider up incrementally increases the Internet security on your computer, so that cookies are not accepted. Moving the slider down incrementally decreases the security, so that cookies are accepted. Check with the IT department for your organisation if you are not sure which settings are appropriate to use.

3. Also in the Settings section, click **Sites** to explicitly set a cookie policy for individual websites. Here, you can specify which sites you want to allow or not allow to use cookies. Enter the desired website address in the **Address of website** text box. Click the **Block** button to block all cookies for the entered site, or the **Allow** button to allow all cookies for the entered site.
4. Continue entering settings for each specific website for which you want to set a cookie policy.
5. Click **OK** to return to the **Internet Options** dialogue box. Click **OK**.

If you are concerned that you may already have cookies on your computer that contain personal information, you can delete cookies and other temporary Internet files by following these steps:

1. In Internet Explorer, on the **Tools** menu, click **Internet Options**.
2. Make sure the **General** tab is selected. (This is the default.)
3. In the Temporary Internet files section, click the **Delete** button. You will be prompted for confirmation before continuing.
4. The Temporary Internet files that you can delete are listed and selected for deletion by default, including **Cookies**. Clear the check box beside any temporary Internet file types that you **do not** want to delete.

5. Click **OK**.



Delete Browsing History

Get more information on privacy features in Internet Explorer 8 (http://windows.microsoft.com/en-US/internet-explorer/products/ie/home?tab=6).

4. Check for encryption before entering information on a site

While surfing the Internet is less dangerous than finding an abandoned bag in an airport, security should still be taken seriously. Encryption is a method that website owners use to help protect sensitive information, such as user names, passwords, addresses, phone numbers, and credit card numbers. If a website you visit does not use encryption, any sensitive information you place on it is easily accessible to hackers who want that information for unsavoury purposes.

There are two ways to ensure you are viewing an encrypted site.

- Make sure you are using the latest version of Internet Explorer as outlined in Tip 1 ("Update, update, update!") above.
- Make sure that a website uses encryption when you are entering or viewing sensitive information. There are two ways to see whether a site uses encryption. One is a small yellow "lock" icon on the status bar of Internet Explorer. The other is in the web address itself. If it begins with **https://** (note the "**s**"), then the site is secure. If you ever visit a website without either of these encryption indicators, do not click a **Submit**, **Save**, or **OK** button, because sensitive information will be transmitted without being encrypted.

Source:
http://www.microsoft.com/atwork/security/research.aspx?WT.mc_id=MSCOM_EN_US_AAN_NEWS_131Z6ENUS22118#fbid=O2KcslwAcgM