CyberSecurity MALAYSIA

An agency under MOSTI

WEB BROWSING

PLAY IT SMART DON'T BE PLAYED!

1. The Great Leap of Web Browsers

These days, web browsers are no longer mere messengers between client and server. They are full-fledged programs capable of using fuzzy logic to select the most appropriate content and help web visitors browse pleasurably and with ease. Today, web browsers have established themselves as the most user-friendly and essential technology tool for surfing the Internet. Web browsers help visitors to the ethereal world of the web to view contents from different file formats, interact with other websites, incorporate appropriate technology to view/download/upload multi-media content, and in streaming multi-media files. Web browsers provide extra functionalities like the blocking of unwanted pop-up advertisements, spyware, phishing attempts and malicious sites. This best practices, however, will focus on the security intricacies of Internet Explorer 8 and the steps taken to invoke the features that would enable certain security measures to be in place while surfing the Internet.

2. How does the Web Browser Function

A web browser is an application that finds and displays web pages. It coordinates communication between your computer and the web server where a particular web site "lives." When you launch your browser and type in a web address (URL) for a web site, the browser contacts that server, requests the web page you asked for, and displays the page on your computer. The browser translates the code (written in a language such as HTML or XML) for the different elements of the page (text, images, sounds) into the appropriate format, and displays the resulting page.

3. Choosing the Right Browser

Despite the fact that a browser is usually included with the installation of your operating system, you are not restricted to that choice alone. There are several factors to consider when deciding which browser best suits your needs including:

- Compatibility - Does the browser work with your operating system?
- Security - Do you feel that your browser offers you the level of security you want?

- Ease of use - Are the menus and options easy to understand and use?
- Functionality - Does the browser interpret web content correctly? If you need to install other plug-ins or devices to translate certain types of content, do they work?
- Appeal - Do you find the interface and the way the browser interprets web content visually appealing?

4. Ensure Your Browser is Protected: Safe Guard Your Computer

Your web browser is your primary connection to the Internet, and multiple applications may rely on your browser, or elements within your browser, to function. This makes the security settings within your browser even more important. Many web applications try to enhance your browsing experience by enabling different types of functions, but these functions might be unnecessary and may leave you susceptible to attacks. The safest policy is to disable the majority of those features unless you decide they are necessary. If you determine that a site is trustworthy, you can choose to enable the functions temporarily and then disable it once you have finished visiting the site. Ideally, you would set your security at the highest level possible. However, restricting certain features may limit some web pages from loading or functioning properly. The best approach is to adopt the highest level of security and only enable features when you require their functionality.

5. The Functionalities are Easy to Understand

Even with these guides, it is helpful to have an understanding of what the different features mean so that you can evaluate the features to determine which settings are appropriate for you. These best practices shows you the most important security features in Internet Explorer 8 that would enable you to understand the safety measures while surfing the net.

5.1 Eliminate Confusion: Master the Terms

Different browsers use different terms, but here are some terms and options you may find;

Zones - Your browser may give you the option of putting web sites into different segments, or zones, and allow you to define different security restrictions for each zone.

For example, Internet Explorer identifies the following zones:

Internet - This is the general zone for all public web sites. To give you the best protection as you browse, you should set the security to the highest level; at the very least, you should maintain a medium level.

Local Intranet - If you are in an office setting that has its own Intranet, this zone contains internal pages. Because the web content is maintained on an internal web server, it is usually safe to have less restrictive settings for these pages. However, some viruses have tapped into this zone, so be aware of what sites are listed and what privileges they are given.

Trusted Sites - If you believe that certain sites are designed with security in mind, and you feel that content from these sites can be trusted not to contain malicious material, you can add them to your trusted sites and apply those settings accordingly. This permits you to verify that the site you are visiting is the site that it claims to be. This is an optional zone but may be useful if you personally maintain multiple web sites or if your organisation has multiple sites. Even if you trust them, avoid applying low security levels to external sites – if they are attacked, you might also become a victim.

Restricted Sites - If there are particular sites you think might not be safe, you can identify them and define heightened security settings. Because the security settings may not be enough to protect you, the best precaution is to avoid navigating to web sites that make you question whether or not they're safe.

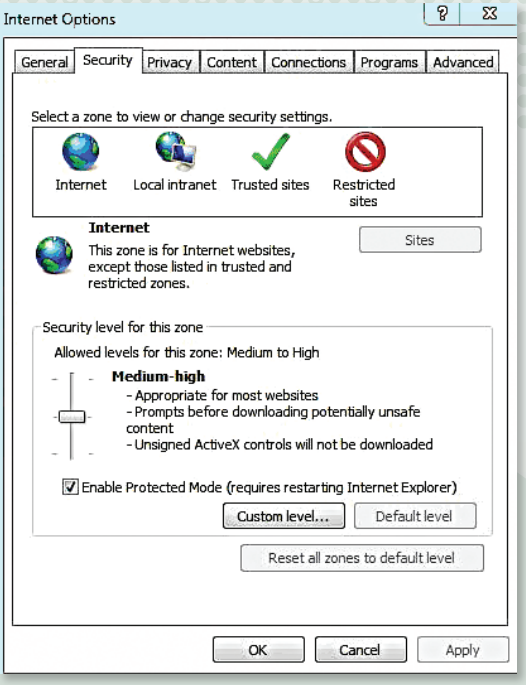

Figure 1 : Zone to view or change security settings

To navigate the following security settings, kindly view the steps as shown in Figure 1. Each web browser is different, so you may have to look around. For example, in Internet Explorer, you can find them by clicking Tools on your menu bar, selecting Internet Options, choosing the Security tab and selecting a zone to view or change security settings.

Steps taken to navigate the segment of zones (Internet, Local Intranet, Trusted sites, or Restricted sites). In Internet Explorer, you can find them by clicking Tools on your menu bar, selecting Internet Options, choosing the Security tab and maneuvering the level of security from Medium to High. By clicking the Custom Level button as shown in Figure 1, you can customise the settings that suits your needs.

5.2 Always Read your Privacy Policy

Before submitting your name, email address, or other personal information on a website, look for the site's privacy policy. This policy should state how the information will be used and whether or not the information will be distributed to other organisations. Companies sometimes share information with partner vendors who offer related products, or may offer options to subscribe to particular mailing lists. Look for indications that you are being added to mailing lists by default, failing to de-select those options may lead to unwanted spam. If you cannot find a privacy policy on a website, consider contacting the company to inquire about the policy before you submit personal information, or find an alternate site. Privacy policies sometimes change, so you may want to review them periodically.

5.3 The Security aspect of Online Surfing

To protect attackers from hijacking your information, any personal information submitted online should be encrypted so that it can only be read by the appropriate recipient. Many sites use SSL, or 'Secure Sockets Layer' to encrypt information. Indications that your information will be encrypted include a URL that begins with "https:" instead of "http:", and a lock icon in the bottom right corner of the window. By making sure a web site encrypts your information and has a valid certificate, you can help protect yourself against attackers who create malicious sites to obtain

your information. You want to make sure you know where your information is going before you submit anything. If a web site has a valid certificate, it means that a certificate authority has taken steps to verify that the web address actually belongs to that organisation. When you type a URL or follow a link to a secure web site, your browser will check the certificate for the following characteristics as show in Figure 2.

1. The web site address matches the address on the certificate
2. Verify the validity of the certificate
3. The certificate is signed by a certificate authority that the browser recognises as a "trusted" authority (you may see names like VeriSign, Thawte, or Entrust)

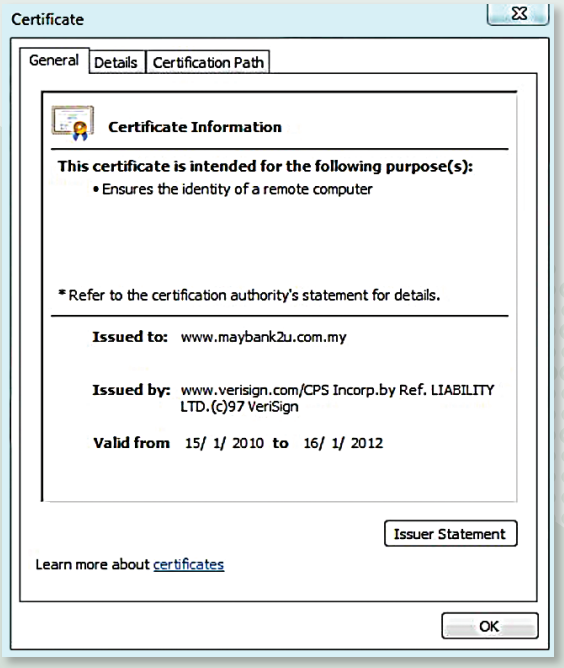

Figure 2 : Maybank2u Certificate Information

Steps taken to view a Certificate

In Internet Explorer, you can find them by clicking Files on your menu bar, selecting Properties, and choosing the Certificates button to verify the validity and authenticity of the site.

5.4 Secure your Confidential Information: Enable TLS & SSL

Never provide confidential (e.g. personal, financial) information while surfing or replying email messages. Use encryption where possible. Ensure Transport Layer Security (TLS) or Secure Sockets Layer (SSL) is used when performing online transactions

or with any information that you reveal online. Below are some steps to follow when sending important information online.

Steps taken to activate TLS & SSL

In Internet Explorer, you can find them by clicking Tools on your menu bar, selecting Internet Options, and choosing the Advance tab. Scroll down to Security and tick on the option SSL 3.0 followed by TLS. 1.0.

5.5 Cookies: Ensure your Information is at your Fingertip to avoid it from being exploited

A cookie is a mechanism that allows the server to store its own information about a user on the user's own computer. You can view the cookies that have been stored on your hard disk. To be more specific, information about your browsing habits such as the last time you visited a particular web site, or your personal preferences for viewing that site. Although the content stored in each cookie may not make much sense to you). To increase your level of security, consider adjusting your privacy and security settings to block or limit cookies in your web. To make sure that other sites are not collecting personal information about you without your knowledge, choose to only allow cookies for the web site you are visiting; block or limit cookies from a third-party. If you are using a public computer, you should make sure that cookies are disabled to prevent other people from accessing or using your personal information.

Steps taken Using Cookies Commands

Enable/Disable Cookies on Internet Explorer 8

1. Cookies are handled very differently in Internet Explorer 8 compared to the older versions of IE Here's how you can enable or disable them.
2. Click Tools.
3. Select Internet Options.
4. Click Privacy.
5. Move the slider to a setting desired. Options range from Block All Cookies or to Accept All Cookies. There are also options under Advanced options where you can customise the settings according to your needs.

5.6 Delete Temporary Internet Files, Cookies and History in Internet Explorer 8

The reasons for this can vary, and in many cases they may be for a personal motive, for security, or something else entirely. Regardless of what drives the need, it is nice to be able to clear your tracks, so to speak, when you are done browsing.

Temporary Internet Files: Copies of Web pages, images and media that are saved for faster viewing.

Cookies: Files stored on your computer by websites to save preferences such as login information.

History: List of websites you have visited.

Steps taken to delete Temporary Internet Files, Cookies and History

1. Click on the Tools menu.
2. When the drop-down menu appears, select the Delete Browsing History option.
3. The Delete Browsing History window should now be visible.
4. Choose any of the options available and click delete.

5.7 Never leave any of your Footprints: Enable InPrivate Browsing

Starting with Internet Explorer 8, it is possible to surf anonymously, without leaving any footprint on the computer. This is particularly useful if what you are using is not your computer and you are afraid to leave your cookies around, which could be retrieved and used by someone to restore your previous email account session or any useful pictures and information. In a Private Browsing session, Internet Explorer will not keep any browser history, search history, download history, web form history, cookies, or temporary Internet files. However, files you download and bookmarks you make will be kept. Always bear in mind that "The Web Should Be Your Safe Playground".

Steps taken to enable InPrivate Browsing

The first way to turn on the InPrivate browsing mode in **Internet Explorer 8** is through its standard options. Just press Ctrl+Shift+P, or just click on Tools in the menu and scroll down to InPrivate Browsing option. You could also scroll down to InPrivate browsing filter to customise the settings according to your needs.

Note: While this computer will not have a record of your browsing history, your employer can still track the pages you visit based on the infrastructure setup and application used.

5.8 Protect yourself from unwanted Pop-ups by enabling Popup Blocker

Although turning pop up blocker feature on this could restrict the functionality of certain web sites, it will also minimise the number of pop-up ads you receive, some of which may be malicious. It also poses very common security issues. Note that "False Perceptions Must Never be Left to Contaminate the Mind, don't be Deceived".

Steps taken to enable Popup Blocker

In **Internet Explorer 8**, you can find them by clicking Tools on

your menu bar, selecting Popup Blocker, and choosing the Turn on pop up blocker.

5.9 Protect yourself from malicious website by enabling Smart Screen Filter

These smart screen filter is designed to protect your computer from malicious websites. Specifically, it is programmed to prevent access to bogus websites that collect personal information while pretending to conduct legitimate business. Always keep your guard and “Stop the thieves from taking advantage of open doors”.

Steps Taken to enable Smart Screen Filter

In **Internet Explorer 8**, you can find them by clicking Tools on your menu bar, selecting Smart Screen Filter, and choosing the Turn on Smart Screen Filter.

6.0 AutoComplete: Injecting Intelligence into a Browser

Would it not be great if you didn’t have to remember 25 different passwords? It can be very frustrating to sit down and try to access your bank web site, your eBay account, or another site you have registered for and try to remember which username and password you used for that account. Internet Explorer offers a feature which can help solve this issue. Unfortunately, it is also a security risk. The AutoComplete feature in Internet Explorer can save web addresses, form data, and access credentials such as usernames and passwords. This information will then be automatically entered every time you visit the site again. The issue is that the credentials will also be automatically entered for anyone else who sits down at your computer and accesses those same sites. It defeats the purpose of having usernames and passwords if they are already automatically entered by your computer. You can control what information the Internet Explorer AutoComplete feature stores, or choose to turn them off.

Steps taken to enable AutoComplete:

1. In an Internet Explorer 8 browser window, click on Tools.
2. Click on Internet Options.
3. On the Internet Options configuration console, click the Content tab.
4. In the AutoComplete section, click on the Settings button.
5. You can select or de-select different types of information to store in Auto Complete.

Note: Use Auto Complete features only on a personal computer

6.1 Iframes: Don't be deceived by the advertisement that appears on the web

To understand an iframe, it is usually helpful to compare it to the generic HTML frame. HTML frames divide the page into separate sections, all populated from different physical pages displayed at once. Users can scroll down one page while keeping another page static, all on the same screen. HTML frames are supported in almost all current browser versions. In totality, they are not evil unless the context in which they are used has been wickedly redefined.

What do iframes look like? If your browser supports iframes, look at Figure 3 for an example:

Figure 3 : Iframe

Malicious iframes planted on compromised websites pose big problems for web surfers. Attackers normally use iframes to trick users into loading malicious scripts. Fortunately, Internet Explorer v6 and above includes a feature that can help protect against malicious iframes. But use this with caution - there are many legitimate uses for iframes and unfortunately IE doesn't distinguish between these.

To ensure a safer surfing environment kindly follow the steps below to disable iframes.

1. Open **Internet Explorer 8**, select Tools and scroll down to Internet Options.
2. Click the Security tab.
3. Choose the desired zone (Internet, Local Intranet, Trusted sites, or Restricted Sites) and click Custom Level.
5. Under Miscellaneous scroll down to Launching programs and files in an IFRAME.
6. Select Disable to prevent iframes altogether or Prompt if you wish to decide on a site-by-site basis.

8. Click OK.
9. Repeat for each of the desired security zones.
10. Click OK to exit the Internet Options menu.

For more information on online support for Internet Explorer 8, kindly visit the following URL;
http://support.microsoft.com/default.aspx

6.2 Keep it Fresh, Keep it Secure, Keep it Updated

Steps taken to enable Automatic Update: A Shield Against Attacks

This is as easy as ABC. Anyone can do this and to ignore it is to invite unnecessary trouble. Enable automatic update for your operating system and application software, and always use the latest version. Go to Start and click on Control Panel and Search for Windows Update Icon, which you can double click and choose your settings on when to perform updates according to time and date.

Another helpful tool is the Personal Software Inspector from security vendor Secunia. It is a free program designed to inform users when their application needs patching and it periodically checks if new updates have been issued for several thousands of other applications. To download this application please visit **https://psi.secunia.com**.

Incident Reporting Channels
Our contact:

Malaysia Computer Emergency Response Team (MyCERT)

E-mail cyber999@cybersecurity.my
Cyber999 Hotline 1 300 88 2999
Fax 603 - 89453442
(monitored during business hours)
SMS CYBER999 Report <Email> <Complaint>
to 15888
H/P 019-266 5850 (24x7 call incident reporting)
Website http://www.mycert.org.my/

CyberSecurity Malaysia
Level 7, Sapura @ Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia

Tel : +603 - 8992 6888
Fax : +603 - 8945 3205

www.cybersecurity.my

Malaysia

MOSTI
Ministry of Science, Technology and Innovation

Best Brand Internet Security

ISMS SIRIM 074 UKAS

CERTIFIED TO ISO/IEC 27001:2005
CERT NO.: AR4656

STANDARDS MALAYSIA
ACCREDITED CERTIFICATION BODY

MS ISO/IEC GUIDE 52:1999
QS 02121999 CB 01

MSC MALAYSIA
Status Company