Protect your Web browser

Today, browsers like Internet Explorer, Mozilla Firefox and Safari ... are installed on most computers. Because browsers are used on a regular basis, the issue of ensuring it is safe is one

This article will help you configure your browser more securely when accessing the Internet. This document is written for home computer users, students, employees in small companies and those with broadband connections (cable modem, DSL, ADSL) or dial-up, rarely get IT support. However, the information in this article can also help people who know more about IT.

I, Why protect your browser

Today, browsers like Internet Explorer, Mozilla Firefox and Safari . are installed on most computers. Because browsers are used on a regular basis, the issue of ensuring it is safe is an important task. Typically, a web browser comes with an operating system that is not set up in a safe default configuration. Failure to secure your browser may result in a variety of problems caused by spyware that compromises your control of your computer.

Ideally, computer users should assess the risks from the software they use. Many computers are sold with downloaded software. Whether installed by a computer manufacturer, operating system, Internet service

provider, or retailer, the first step in accessing your computer is to find out what software is installed. and how a program interacts with other programs. However, most people do not perform this level of analysis.

Today the number of attacks aimed at the weaknesses of the browser is increasing. It has been observed that software is directly attacked in browsers by using dangerous websites. This issue is assessed according to some of the following issues:

1. Browsers are configured to provide many functions but with reduced security features.
2. New security vulnerabilities can be detected when the software is configured and packaged by the manufacturer.
3. Many websites require users to activate key features or install more software, making your computer more risky.
4. Many people do not understand how to configure their web browsers to be safe.
5. Many people are not willing to enable or disable the functionality required for browser security.
6. Many people do not understand whether their computers are at risk.
7. Many people fail with a compromised computer.

Finally, exploiting vulnerabilities in browsers becomes popular for attackers to harm your computer.

II, Learn the features of the browser

Understanding browser functions and features is an important issue. By activating several browser features can reduce security. For example, the ActiveX software feature has many vulnerabilities that can greatly affect security.

Many browsers can be installed on your computer. Other software applications on your computer such as email software or text reader software can use another browser that is not the browser you use to access the web. Likewise, specific file types are configured to open with another browser. By using a browser to access the site does not mean that the remaining applications will automatically use the same browser. For this reason, it is very important for secure configuration of each browser installed on your computer.

Websites that may require the use of a browser that supports scripting or Active components such as JavaScript or ActiveX controls or pages themselves may also have vulnerabilities. Websites can be thought of as products and user relationships with products, you can contact webmasters and ask how pages should be designed to pose no risk. for your computer.

Some features and attributes of some specific browsers are described in this document. Understanding what features will help you know how they affect the functionality of your browser and your computer's security.

Source: browserhelp.de **ActiveX** is a technique used by Microsoft Internet Explorer on Microsoft Windows. ActiveX allows applications or application parts to be used by web browsers. A website may use ActiveX components that reside on a Windows system or may download that component depending on a website. This has allowed the functionality of the traditional browser to be extended, but it also caused some security holes if not added in a timely manner.

Java is an object-oriented programming language that can be used to develop content for websites. Java Virtual Machine or JVM is used to execute Java or 'applet' code provided by the website. The JVM is designed to separate the executable code so as not to affect the rest of the system. Some operating systems support a JVM while other operating systems require the JVM to be installed before using Java. Java applets run completely independent of operating systems.

Active Content or Plug-ins are intended for use in the browser. They are like ActiveX controls but cannot be executed outside the browser. Macromedia Flash is an example of Active Content that can be provided as a plug-in.

JavaScript is a dynamic scripting language used to develop content for pages. Unlike Java, JavaScript is a language that is interpreted directly by the browser. There are many details in the JavaScript standard that restrict features such as accessing local files.

VBScript is a scripting programming language of Microsoft Windows. VBScript is like JavaScript but it is not widely used in pages because of its compatibility with other browsers unlike Internet Explorer.

Cookies are text files that are placed on your computer to store data already used in a web page. A Cookie may contain any information depending on the design purpose of the website. Cookies may contain information about

the pages you have visited or even include the ability to access. They are designed to be read only by a website that creates them.

Security Zones and Domain Model are Microsoft Windows methods used designed to establish multiple layers of security for systems. While the main purpose is used for Internet Explorer, it may also be necessary for other applications on the system to use IE components. You can find out more about Security Zones, Domain Models and how to protect them at: http://www.microsoft.com/windows/ie/using/howto/security/setup.asp.

III, Vulnerabilities and types of attacks

Attackers are exploiting the client system (on your computer) through various vulnerabilities. They rely on these vulnerabilities to gain control of your computer and then steal information, destroy files and attack other computers. One effortless way for attackers to increase control on your computer is to exploit vulnerabilities in web browsers. An attacker can easily create a dangerous website then install Trojan or spyware software to steal information from your computer. You can see more details about spyware at http://www.us-cert.gov/reading_room/spyware.pdf. More dangerous than attacking system vulnerabilities, a malicious website can harm systems passively as the site was visited previously. A dangerous HTML document can also be dangerous for many victims. In this case, opening an email or attaching an attachment may damage the system.

In this section, we will point out some common vulnerabilities in web sites and browsers that have been exploited. We will not go into specifics but will provide you with links in other documents to explain more about the vulnerabilities.

A, ActiveX controls

ActiveX is a technology that causes many different vulnerabilities. One problem with using ActiveX in a browser is that it has increased the attack surface, or 'attack capability' for the system. Vulnerabilities in ActiveX objects can be exploited via Internet Explorer, even if the object is not designed for use in a browser. In 2000, CERT / CC helped a workshop for security analysis in ActiveX. Results from that analysis can be found at http://www.cert.org/reports/activeX_report.pdf. Many vulnerabilities are related to ActiveX controls. The attacker here by exploiting these vulnerabilities can increase the control of computers. You can find pages about ActiveX vulnerabilities in the following links http://search.us-cert.gov/query.html?qt=activex and http://search.cert.org/query.html? qt = activex.

B, Java

Java is an object-oriented programming language developed by Sun Microsystems. The Java applet is completely independent and requires a Java Virtual Machine (JVM) on the client so it can be executed. Java applets often execute within a 'location' where interaction with the rest of the system is limited. However, the JVM contains many vulnerabilities that allow an applet to overcome these limits. Authenticated Java applets can also overcome many of these limitations, but in general they prompt users before they execute. You can search on US-CERT and CERT / CC pages to see more about these vulnerabilities at http://search.us-cert.gov/query.html?qt=java and http:/// search.cert.org/query.html?col=certadv&col=vulnotes&qt=java.

C, Cross-Site Scripting

Cross Site Scripting allows an attacker to embed malicious code: Javascript, VBScript, ActiveX, HTML or Flash into an attackable dynamic page to trick users into activating the code on his or her computer for collection. data collection.

Hackers are always experimenting with a cunning script of hacking techniques to harm websites and web applications and steal the useless treasure of vulnerable data including credit card numbers. and other personal information.

Cross Site Scripting (also known as XSS or CSS) is believed to be one of the most popular applications of hacker trap techniques.

Overall, cross-site scripting is a lever for vulnerable features in web application code that allows an attacker to send malicious content from a user object and retrieve the victim's data.

D, Cross-Zone and Cross-Domain vulnerabilities

Most browsers use security models to prevent data access to another domain from a website. These security models rely heavily on Same Origin Policy Netscape: http://www.mozilla.org/projects/security/components/same-origin.html. Internet Explorer also has a measure to divide this security zone: http://msdn.microsoft.com/workshop/security/szone/overview/overview.asp.

Vulnerabilities in this security model can be used to perform unusual actions. The impact may be the same as the cross-site scripting vulnerability. However, if the vulnerability allows an attacker to hack into a local area or other protected area, the attacker can execute arbitrary commands on the system. You can find more information in the US-CERT and CERT / CC pages at the following address: http://search.us-cert.gov/query.html?qt=cross-domain and http:/// search .cert.org / query.html? qt = cross-domain.

E, Threats from Script scripts, Active and HTML components

Many pages may contain dangerous script code, Active or HTM components. They will try to deceive visitors to provide good information to implement Phishing Techniques (Social Engineering: A term derived from the information technology world, referring to the deception of computer users and Internet disclosures). In order for a hacker to gain access to the system, the most common way of doing this is to contact the victim through chat or e-mail, pretending to be a security officer. is checking and asking users to declare their password to authenticate their identity or their account will be closed, allowing an attacker to increase privileges. In that opportunity, attackers rely on phishing techniques to access the victim's information. In addition, vulnerabilities in browsers can be exploited to increase privileges. Below is a list of possible vulnerabilities in browsers through the use of malicious code. In 2000, CERT / CC came up with a series of answers about malicious scripting. You can refer to http://www.cert.org/tech_tips/malicious_code_FAQ.html. And see more articles on this issue at http://search.us-cert.gov/query.html?qt=malicious+scripting+active+content and http://search.cert.org/query.html? qt = malicious + scripting + active + content.

F, Phishing-type scam (Spoofing)

When it comes to browsers, spoofing is a term used to describe browser interface spoofing methods. This includes an address or location bar, status bar, keychains, or other user interface components. Information theft attacks, especially credit card information, often use a few fake forms for users to trust and provide personal information. If the browser lacks this error, the user will become a victim of this phishing attack. This is a simple but quite effective attack method so be careful before any unreliable link sent to you requires updating your account information.

Please read the following article: **Security for Microsoft Internet Explorer**

You finished reading the article "**Protect your Web browser**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.