Guidelines on using a Web browser

Center for Information Technology, Kansai University

1 Purpose of these guidelines

Web browsers are now indispensable tools for delivering and sharing information. However, Web browsing and unauthorized posting on bulletin board systems could cause the university to lose the trust of society.

The purpose of these guidelines is to reduce these risks, protect information assets, and specify what is necessary for users to safely and securely use Web browsers.

Additionally, it is recommended to have antivirus software installed on PC terminals used for Web browsing.

2 Intended audience for these guidelines

(1) Audience

The intended audience for these guidelines includes all users who use the network services provided by the university to use Web browsers (hereinafter referred to as “users”).

3 General precautions about using Web browsers

To ensure the safety of users when using Web browsers to visit Websites and when using various information systems, general precautions about Web browsers are provided.

(1) Prohibited use other than use for intended purposes

1) Users shall visit Websites to the extent that it is necessary to engage in research, educational, and educational support activities at the university. They shall not do so for any other purposes. Use of the network for commercial purposes is prohibited.

2) Users should keep in mind that by visiting any Website from within the university, the domain name and IP address of the university will end up being recorded. Based on recorded information, server administrators may make undue requests to the university or request that viewers’ personal information be disclosed. Additionally, if you enter your name or email address, you could be charged with false claims.

(2) Restricted Website access

1) To maintain proper Web usage, Website access may be restricted by content filtering. Users shall be aware that access to Websites they wish to visit may be restricted.

2) Users shall be aware that they need to hold themselves responsible for accessing Websites even if such Websites are not restricted by content filtering.

3) When users want to visit restricted Websites, they shall contact the Center for Information Technology for assistance.

(3) Precautions when installing and using plug-ins

1) Users shall be aware that by installing and using plug-ins (software to enhance Web browser features) not regarded as acceptable for use by the Center for Information Technology, security may be lowered.

2) When users need to install and use plug-ins not regarded as acceptable for use by the Center for Information Technology, they shall contact the center for assistance.

(4) Precautions when using services provided by external Websites

1) Users shall take extra care when posting on external bulletin board systems or to blogs and using Web mail services.

2) Do not post anything inappropriate or use such services in an inappropriate manner that is against public order or morality. Even short posts on bulletin board systems could cause people to doubt the sense of the university or its members. In particular, do not post anything that could be mistakenly interpreted as a defamatory statement or that would cause doubts to arise concerning infringement of privacy or copyrights.

3) There are many links on the Internet that are designed to direct users to unauthorized Websites or make them download unauthorized software such as viruses. Even well-known Websites may not be secure.

(5) Monitoring Website access

1) To maintain proper Web usage, usage logs (e.g., records of who visited which Website and when) may be obtained, stored, inspected, and analyzed. Users shall understand such purpose and be aware of the fact that their own Website viewing activity is being recorded.

4 Web browsing

Instructions on how to use Web browsers for Web browsing and precautions to prevent possible threats associated with Web browsing are provided.

(1) General precautions about Web browsing

1) Users shall keep in mind the following when visiting Websites:

i) Information on Websites could be not only correct but also false or wrong. Do not accept it as is without scrutinizing it.

ii) Refreshing a Web page repeatedly over a very short period of time could be considered to constitute a Denial of Service (DoS) attack (an attack intended to produce unwanted communication within a service to decrease the quality of that particular service). Depending on Websites, the domain or IP address of the university could be blocked. Access could also be blocked even by a temporary download of a large number of online journals, making it impossible for other users to access such online journals. Take extra caution when doing so.

iii) Links to malicious Websites could be included in search results of Websites. Do not easily access links in search results. The order of a search result does not represent the level of information reliability, either.

iv) Even ads posted on well-known Websites could be linked to malicious Websites or virus download sites. Do not easily click ads.

v) Do not easily click links in HTML email. This could direct you to impersonating Websites or one-click fraud Websites, or result in fraud damages. Do not download software even if prompted to do so with an unfamiliar security warning when viewing Web pages. You could be forced to download viruses or unauthorized software.

(2) Checking TLS (SSL) communication

1) TLS (SSL) [1] communication is secure communication for which measures are taken to encrypt communication and counteract impersonation attacks. This technology is used as a standard on Websites that send and receive important information. Users shall make sure that URLs of Websites they are visiting start with “https://,” if these Websites are possibly sending and receiving personal or important information. At the same time, make sure that the certificate shown is legitimate. Note, however, that some certificates can be obtained at low prices by anyone. You shall take extra care even if a certificate is legitimate.

(3) Measures against confirmation/warning dialogs

1) Depending on security-related settings, confirmation dialogs may be displayed. If you easily allow scripts such as ActiveX® and Java® to be executed against the university’s software, it poses the risk of information disclosure. Users shall not easily allow such scripts to be executed without checking what they are, if a confirmation dialog is displayed.

(4) Viewing Websites that request Web browser settings to be changed

1) Users shall not easily change their Web browser settings that are related to plug-in/script execution, if requested to do so by Websites so that they can view these Websites. This could decrease the security level and pose the risk of infection with unauthorized programs.

5 Sending information to Websites (sending information entered in forms, uploading files, and the like)

Precautions to prevent possible threats associated with eavesdropping on information being sent, sending information to a wrong recipient by impersonation, or sending information to other Websites are provided.

1) Use a safe, secure communication channel such as TLS (SSL) for sending important information. At the same time, make sure that the relevant certificate is legitimate.

2) When entering information, be aware of risks posed by Cross-Site Scripting (XSS) attacks. Access pages that require entry of information not via portals but rather via links available on the same Website where forms exist.

6 Downloading files

Precautions to prevent possible threats associated with executing or opening files downloaded from Websites are provided.

(1) Restrictions on executing executable files and opening document files

1) Viruses can be detected by the automatic scanning feature of antivirus software, if an executable file is executed directly from a Web browser. However, when downloading

[1] A major vulnerability has been found in SSL (Secure Sockets Layer). Because of this, as of 2015, TLS (Transport Layer Security) was commonly used as the successor to SSL. However, expressions such as “connect over SSL” are still used for encrypting communication with Websites.

executable files, it is desirable that users check them for electronic signatures or unauthorized programs. Also, to make it easy to identify files that have caused trouble if such trouble occurs, it is desirable that users download (and save) executable files on PCs and then execute them, instead of executing them directly from a Web browser.

2) Viruses can be detected by the automatic scanning feature of antivirus software, if a document file is opened directly from a Web browser. However, when opening (or using) document files on Websites, it is desirable that users check them for electronic signatures or unauthorized programs. Also, to make it easy to identify files that caused trouble if such trouble occurs, it is desirable that users download files on PCs, instead of opening them directly from a Web browser. (Provided, however, that this shall not apply in cases in which users attempt to open [or use] document files on trusted Websites.)

3) If downloaded executable files are not listed as programs regarded as acceptable for use by the Center for Information Technology, users shall take extra care when installing and using them.

(2) Checking saved files for unauthorized programs

1) Before executing saved files or opening particular software, users shall make sure that they are not unauthorized programs.

2) When users find that unauthorized programs are included among saved files, they shall contact the Center for Information Technology for assistance, without executing such files or opening particular software.

(3) Checking saved executable files for electronic signatures

1) When users can identify the distributors of saved executable files, they shall make sure that such distributors are appropriate organizations.

(4) Measures when PCs are infected with unauthorized programs

1) When users' PCs became infected with unauthorized programs because they have executed or opened downloaded files or when there is a suspicion of the same, users shall isolate their PCs from the network by immediately disconnecting LAN cables or shutting off wireless connections, and then such users shall contact the Center for Information Technology for instructions.

7 Contact for these procedures

(1) If users need to cope with emergencies or take measures beyond the scope of these guidelines, they shall contact the Center for Information Technology for assistance.

(2) If users have any questions about the content of these guidelines, they shall contact the Center for Information Technology.

Supplementary provisions

1. These guidelines become effective on November 6, 2019.