How to Tighten Your Browser's Security

Share - from AOL.Discover

Click here: How to Tighten Your Browser's Security

One of the most basic ways to protect your computer from potentially harmful online content or malicious software is easy, fast and free. How? Just make sure your browser's security settings are set at the appropriate level.

No matter which browser you use, always follow these top five security tips:
1. Delete spam messages without opening them or replying to them.
2. Use great caution when clicking on links sent to you in e-mail or text messages.
3. Do not open e-mail attachments unless you know the sender and you're expecting the attachment.
4. Create strong passwords. Use different passwords for your online banking accounts.
5. Make sure you use a firewall, as well as antivirus and antispyware software that is automatically updated.

What are the security settings on your browser? Here's how you can find out in Internet Explorer and Firefox.

How to check your Internet Explorer security settings:
1. Open Internet Explorer.
2. Click the Tools button and then click Internet Options.
3. Click the Security tab.

You will see four security zones:
• Internet: The level of security for the Internet zone is applied to all Web sites by default. The security level for this zone is set to medium-high, but you can change it to either medium or high. The only Web sites for which this security setting is not used are those in the Local Intranet zone, or sites that you specifically entered into the Trusted or Restricted Site zones.

• Local Intranet: The level of security for the Local Intranet zone is applied to Web sites and content that is stored on a corporate or business network. The security level for the Local Intranet zone is set to medium, but you can change it to any level.

• Trusted Sites: The level of security for Trusted Sites is applied to sites

that you have specifically indicated to be ones that you trust not to damage your computer or information. The security level for Trusted Sites is set to medium, but you can change it to any level.

- Restricted Sites: The level of security for Restricted Sites is applied to sites that might potentially damage your computer or compromise your personal information. Adding sites to the Restricted zone does not block them, but it prevents them from using scripting or any active content. The security level for Restricted Sites is set to high and cannot be changed.

As you move around the Internet, IE automatically changes the security zone as needed and sets your security level for each Web site by default, ranging from low or medium-low for a corporate Intranet site, to high for a restricted site.

How to view or change the security settings on Internet Explorer 7/8:
In addition to these default security levels, you can customize individual security settings.

1. Open Internet Explorer.
2. Click the Tools button and then click Internet Options.
3. Click the Security tab.
4. Click the "Custom level..." button.
5. At the bottom of the pop-up box, you can reset the security setting to something higher or lower. Settings that are not at recommended levels will be highlighted in red.
6. If you modify your security settings and want to change them back to the default level, follow the above instructions through step 4. Then click on the "Reset all zones to default level" button.

How to view or change the security settings in Firefox 3x:
To make sure your security settings offer you the most protection, do the following:

1. Open Firefox.
2. Click on the Tools button and then click Options.
3. Click on the Security tab.

Step 1: Make sure the first three blocks are checked:

- Warn me when sites try to install add-ons.

Firefox will always ask you to confirm installations of add-ons. To prevent unrequested installation prompts that may lead to accidental installations, Firefox warns you when a Web site tries to install an add-on and blocks the installation prompt.

- Block reported attack sites.

Firefox will check whether the site you are visiting may be an attempt to interfere with normal computer functions or send personal data about you to unauthorized parties over the Internet.

• Block reported Web forgeries.
Firefox will actively check to determine whether the site you are visiting may be an attempt to mislead you into providing personal information, often referred to as "phishing."

Step 2: Passwords
Firefox saves your passwords by default, but if anyone else ever uses your computer, turn this feature off to protect your password security. To do this:
1. Open Firefox.
2. Click on the Tools button and then click Options.
3. Click on the Security tab.
4. Uncheck "Remember Passwords for Sites."

If you share your computer with others, you can set a Master Password in Firefox. This allows you to keep secure the username and passwords of Web sites you visit so no one else but you can access this information. To set a Master Password:
1. Open Firefox.
2. Click on the Tools button and then click Options.
3. Click on the Security tab.
4. Click "Use a master password." You'll be prompted to enter a password. (You can also follow these steps to change your Master Password.) A password-quality meter will judge the security of the password you have chosen.

IMPORTANT: Make sure you remember your Master Password! Without it, even you will not be able to access any of the information it protects or change the password.

Step 3: Warning Messages
1. Open Firefox.
2. Click on the Tools button and then click Options.
3. Click on the Security tab.
4. Click the Settings button that appears to the right of "Choose which warning messages you want to see while browsing the web."
5. At minimum, make sure the box is checked for "I am about to view a page that uses low-grade encryption."

Revised 7/16/2010 JMM