

Safe web surfing rules for the year 2021

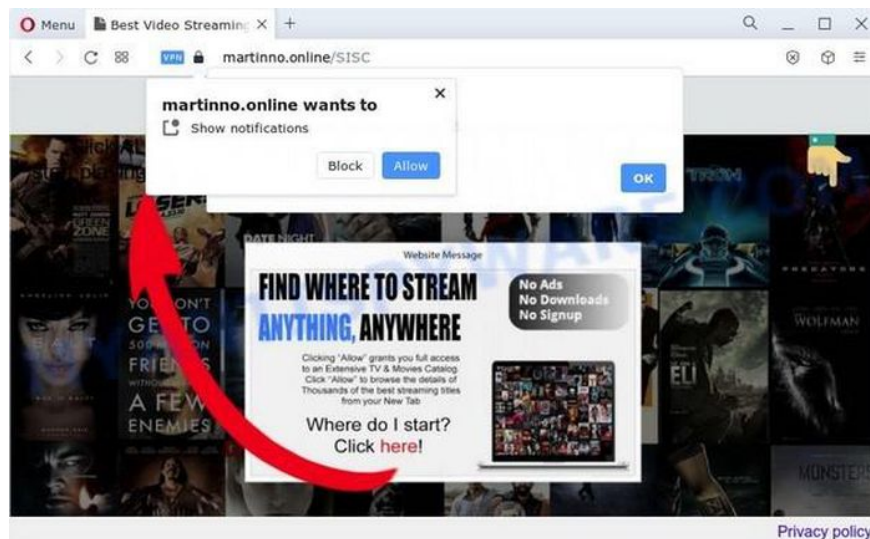
1/5 of the 21st century has passed and there are safe surfing rules that users need to quickly update. Remember the following 11 rules to protect yourself online

1. Point to trusted websites

It is difficult to know which websites are trustworthy and which are not. But technologically, websites with domains beginning with https (not http) are typically significantly more secure. These are the new generation of web application security standards and although not completely secure, but at least it also makes users feel more secure.

2. Don't go to web filled with advertising

No matter how attractive a website's content is, inserting an innocent ad is the first sign that the site is intended to trick users (clickbait). If you encounter websites that automatically open a new tab, pop-up frames take up half of the screen, it is best to exit these websites to avoid pressing the wrong adware.



Stay away from fake web full of pop-up ads and notifications demanding notifications

3. Delete Flash

Adobe officially stopped supporting Flash on December 31, 2020, in the next two weeks any Flash content will be completely blocked. To avoid being exploited for vulnerabilities from this platform, users need to delete Flash

immediately.

In case accessing any website requires Flash reinstallation, it is best for users to ignore that message.

The same is true of Internet Explorer, which has been discontinued by Microsoft since November 2020 and should be removed immediately.

4. Don't download anything in a hurry

Today's modern browsers allow you to preview the content of text files, but many compressed files do not. This means you have to download and then unzip to view the contents.

However, this is a very simple trap that hackers often set up, enticing users to download something seemingly necessary. The rule here is in no rush to download such things.

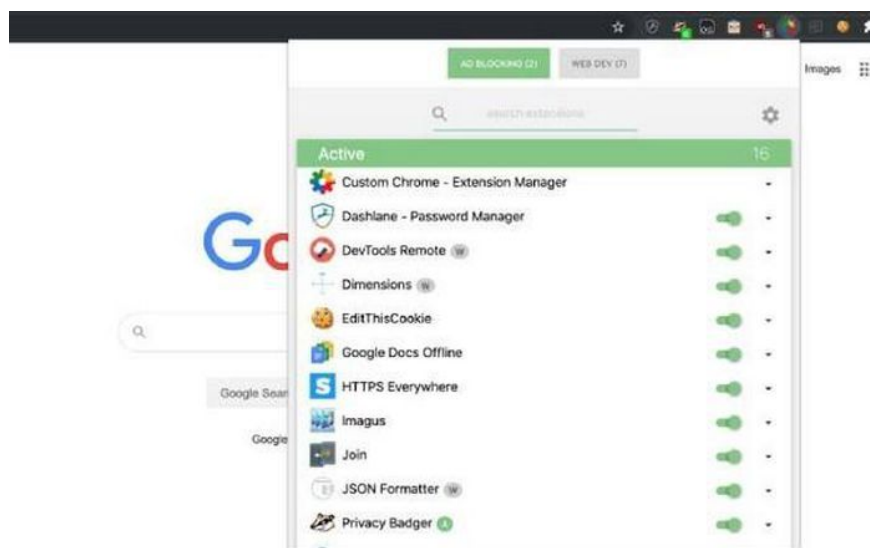
5. Don't trust gifts

If one fine day is surfing the web, you suddenly get a winning message. Please carefully check the sender name, content and how to receive the reward. Because 99% of this is a very basic scam of hackers. The principle here is that nothing can fall from the sky.

The same applies if you get a warning about a virus infection. All ads of this type are fraudulent and have no value.

6. Do not install bluff extensions

Extensions are an integral part of the open browser, especially the ad-blocking extensions. But many of these can be changed at any time and include malicious code without the user's knowledge. Therefore, please limit the use of extensions to the maximum.



Too many extensions can slow down the browser, affecting the user's surfing speed

7. Don't share passwords

It's 2021 and if you still share passwords or weak passwords, you're probably out of date. Reasons like I can't remember dozens of passwords are unacceptable. Use the password manager software / application immediately for web login and write down important security questions.

8. Update anti-virus software

Malware types are growing more sophisticated and unpredictable than ever before. Therefore, an up-to-date anti-virus software has the same value as not being used.

The same is true for web browsers. Regular updating will help limit security vulnerabilities and help users be more secure.

9. Anonymity is not really anonymity

If you are afraid of being crawled by Google or a website and using an incognito browser to dodge it, you should be aware of the fact that this mode only helps not to save history on your device. The actual data is still taken away and sent back to the places you visit, such as the dark web, hacker forums.

To avoid getting crawled, the only way out is to use a VPN or a secure browser that connects via a proxy.

10. Do not enter personal information indiscriminately

Personal information of each person today is of great value in cyberspace. Do not rush to trust sales sites that ask to leave a phone number for advice. Don't rush to give your names and contacts to untrustworthy websites.

Contact first if it is via email and website owner must provide a full range of communication channels (online and offline) for customers to actively contact. Being carefree about your phone number will result in spam text messages and spam calls torturing you every day.

11. Social media accounts are very important

Today things like Facebook or Google (YouTube) accounts are of no small value that many people are not aware of. Therefore, careful care is paramount. But most of all, many people often use the single sign-on feature on third-party websites through this account.

This utility helps users not have to waste time logging in, but the downside is that the website administrator will now grasp at least the login token and personal information through your consent (unconsciously). for that website to crawl. Therefore, please minimize the use of quick login features and take some time to register a new account. If the site is not important, use inaccurate personal information to avoid future disclosure.

You finished reading the article "**Safe web surfing rules for the year 2021**" 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.
