In such uncertain and insecure times, the least that can be done to enjoy anonymous web browsing is to make sure not to leave a digital trail of your activities for hackers and scammers to pick up.

Here are the ten commandments of online safety that you must follow in order to remain secure.

1. Cybercriminals keep coming up with new ways and techniques to make people fall for the scam they create. Make sure you read up about the latest scams once or twice a month. Just Google "**how to browse safely**."
2. Never click on any links that you don't totally recognize and trust. Links that appear in emails sent to you by strangers are to be avoided at all costs. Such links can lead you to websites that can extract personal data from your computer without your knowledge and consent. Also, be over judgmental about suspicious emails you receive from your friends, in which they don't sound like themselves. For example, is your friend suggesting that he's in big trouble and urgently needs you to send him some money? Beware, your friend's account may have been hacked.
3. Online shopping can make you pay for ghost products. Multiple fake websites have been spotted across the internet that looks just like an average online shopping website. The realism dies right after you are make a purchase. Always make sure that the website has a padlock icon (or https) in its URL.
4. Wi-Fi router at your home must be password-protected. This is to make sure that only trusted users are connected to the network.
5. Step up your password game. Gone are the days when BroCode420 was considered a strong password. Now, a strong password must contain small letters, capital letters, numbers, and even special characters. It becomes more difficult to remember such a strong password, but it's still better than getting your account hacked. Always use a different password for each of your accounts. Keep changing or rotating them, say every six months. For more tips on how to create strong passwords, go to **http://passwordday.org/**
6. Browse the **internet safely** and beware of phony websites. You may have heard about a lot of fake news websites during the recent US presidential elections. What many people don't know is that fake websites expand to hundreds of other categories as well, apart from news and media. Some of them even look like a real and reputed website but contain only minor discrepancies, such as a misspelled URL, or a differently spelled brand name. Whenever any website asks for personal information, such as your account details or contact information, make sure the website is authentic.
7. Improve your system security. Keep your devices and machines equipped with strong malware protection software such as antiviruses and VPNs. This can greatly reduce the chances of your device being hacked or infiltrated. It also allows you to browse without being tracked.
8. As a contingency security plan, back up your important data at least once a month, just for the rainy days. It is also a good idea to check your bank statements regularly for any suspicious activity – such as changes in your registered authorization details i.e. email address or mailing address – without your permission.
9. Install a strong firewall. This can prove to be a savior against cyber-attacks and hacks. Though firewalls are now embedded in most OS, it's always better to have a specialized piece of software just for the purpose.
10. Use common sense. You don't need to be a computer genius to understand that a prince from Dubai who wants to give you a million Dirhams is not a prince but a scammer who wants to fool you into giving him some money.