D.A.V PUBLIC SCHOOL SECTOR-14, GURUGRAM

Issue 4: 29 January 2022

SECURING YOUR BROWSER

#CyberSafetyAwareness #SafeBrowsing

ONLINE SAFETY

Remote working presents new and unique challenges for information security. Securing the browser is the first step that needs to be taken in order to assure online protection.

WEB BROWSER RISKS

- Spyware getting installed on computer without the user's knowledge
- Websites can remember your login information, interests which can be used for sending you recommendations
- Phishing scams may force you to reveal your personal information by displaying pop-up windows.
- Malicious code can be inserted that can take control of the browser by allowing it to access system files.

WHAT CAN POSE THREAT?

Pop-ups, Scripts, Plugins, Browser Extensions, Cookie

COOKIES

A cookie is used to identify a website user. A cookie is a small piece of text sent to a browser by a website that is visited from it. It contains information about that visit like remembering the website visited preferred language and other settings. The browser stores this data and uses it in accessing the features of the website or the next time the same site is visited to make the access more personalized.

If a website uses cookies for authentication, then an attacker may be able to obtain unauthorized access to that site by obtaining the cookie.

BROWSER EXTENSIONS

Browser Extensions let you add new features to your browser. For example, you may install a currency converter extension that shows up as a new key next to your browser's address bar. Click the button and it converts all the prices on your present web page into any currency that you give.

Adding more code to the browser also adds to security concerns, as it gives attackers more chances to exploit the browser.

USING BROWSER EXTENSIONS CAUTIOUSLY

- Research an extension's publisher and history before you download an extension.
- Stay alert and observant about your downloaded browser extensions, and delete unused extensions.
- Make sure that the extensions you install come from official repositories, such as the Chrome Web Store or the Firefox Browser Add-Ons portal.
- Pay attention to the permissions that extensions require. If an extension already installed on your computer requests a new permission, that should immediately raise flags; something is probably going on

HOW TO SECURE YOUR WEB BROWSER

1. Configure your browser's security and privacy settings
2. Disable extensions that ask for permissions or look suspicious
3. Disable saved passwords in browsers and disable Autofill
4. Using a strong antivirus and keep it updated.
5. Keep the Operating System and Web browsers up-to-date.
6. Use browser extensions cautiously
7. Work in incognito mode on a public computer so that browsing history and/or logins are not stored
8. Avoid Public Wifi Connections for transactions or other confidential work
9. Regularly change your passwords in different web applications /websites

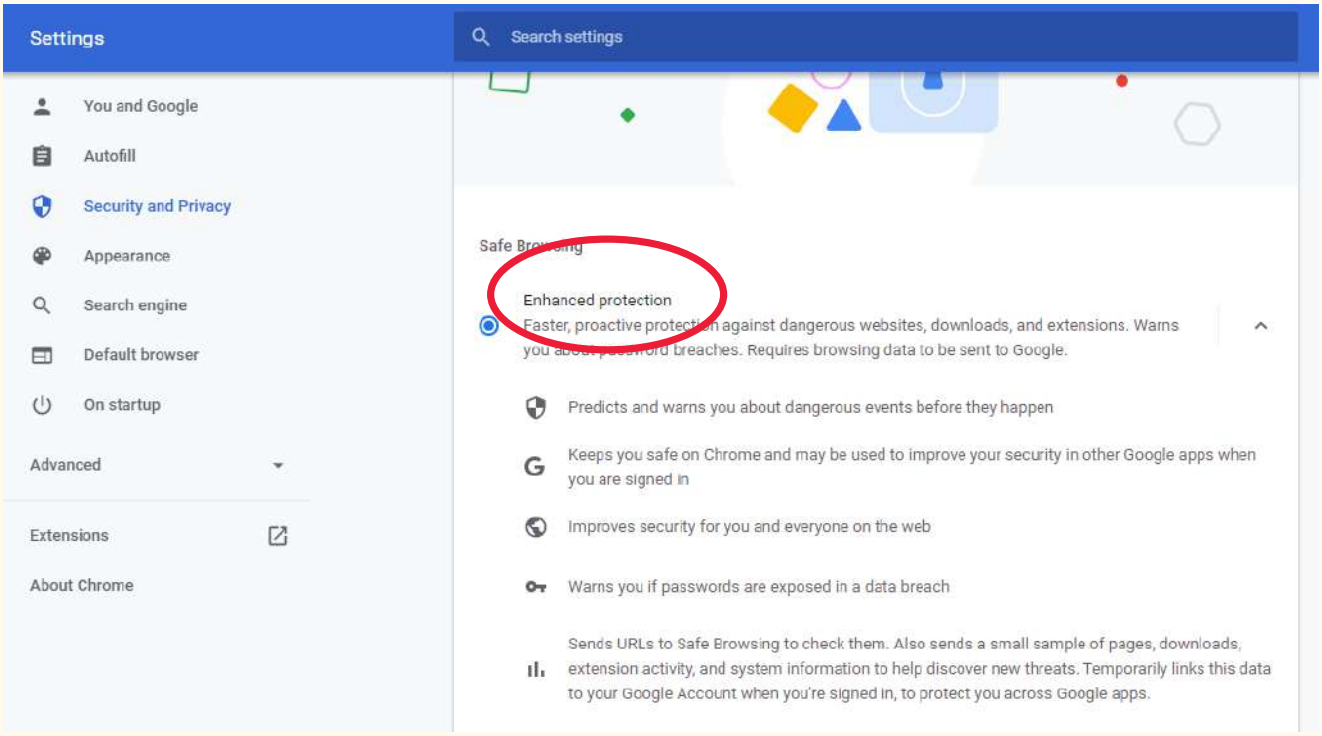
SECURITY TAB

The Security Tab in a Web Browser lets you secure the browser and offer to trust the people, companies on the Internet. This helps to decide and adds which sites to be allowed to run the application, scripts, add-ons, install the plug-in on your computer. Security Tab also contains other features like adding the address of websites under restricted sites.

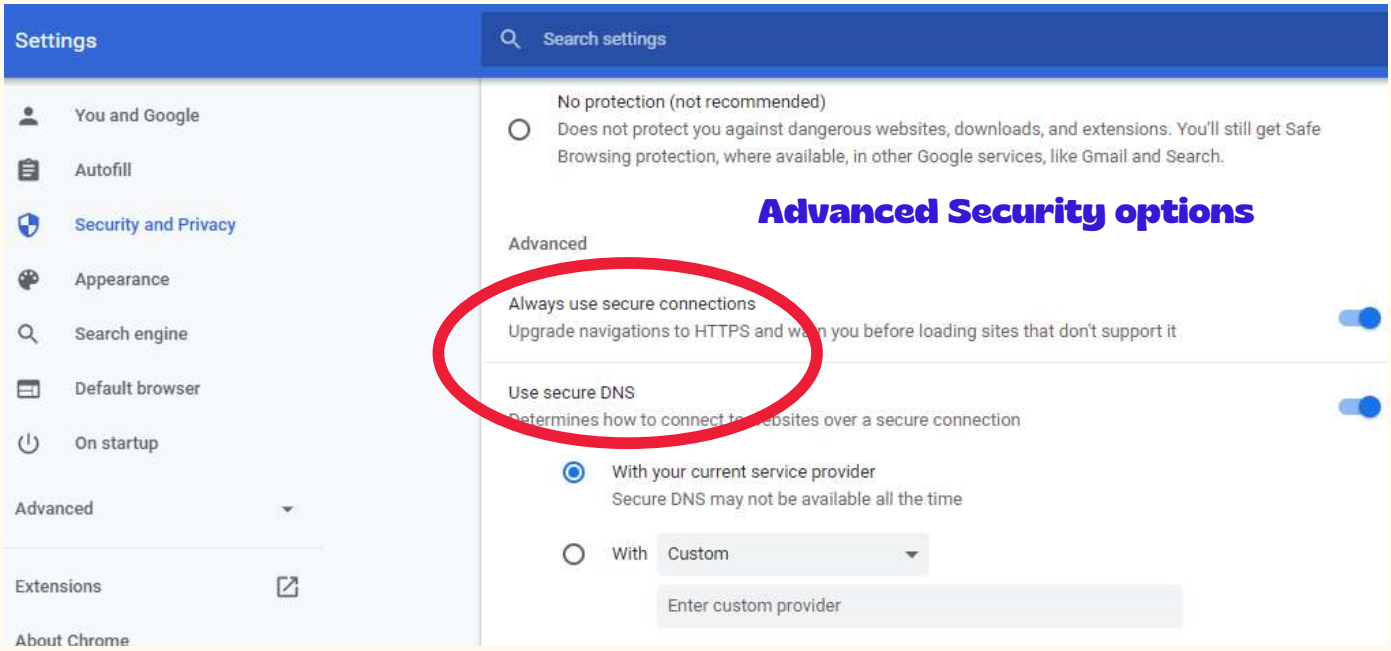
FEW IDEAL SETTINGS

GOOGLE CHROME

Enable Enhance Protection

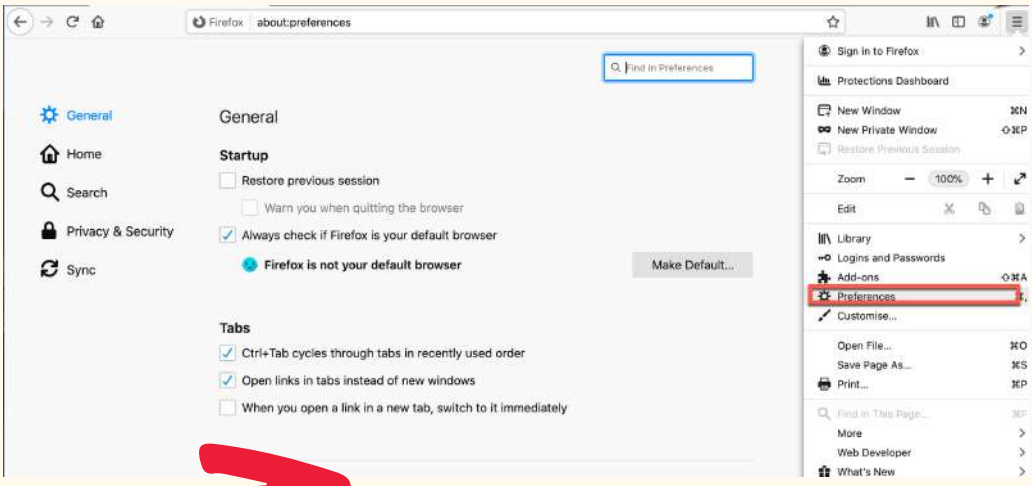


Three dot menu-> Settings-> Security and Privacy-> Enable Enhanced Protection



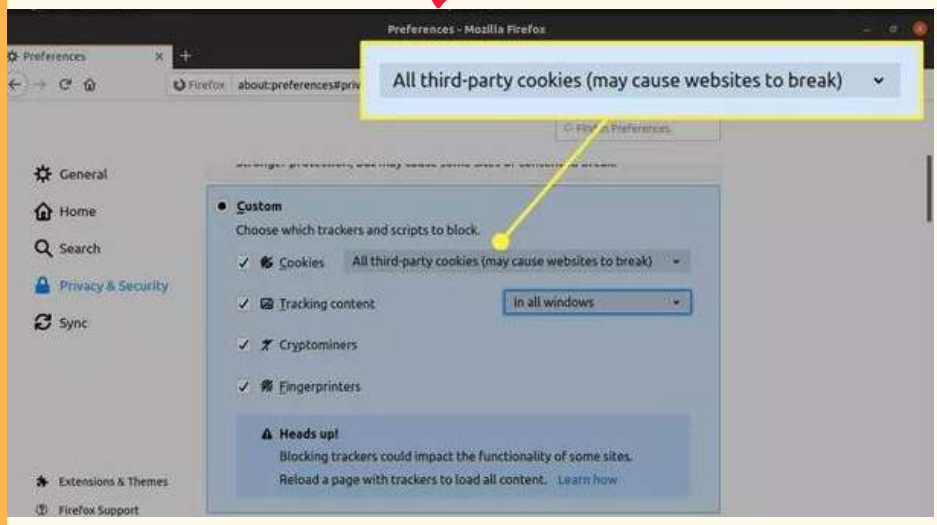
Three dot menu-> Settings-> Security and privacy-> Scroll down-> Under Advanced, enable 'Use secure DNS' and 'Always use secure connections.'

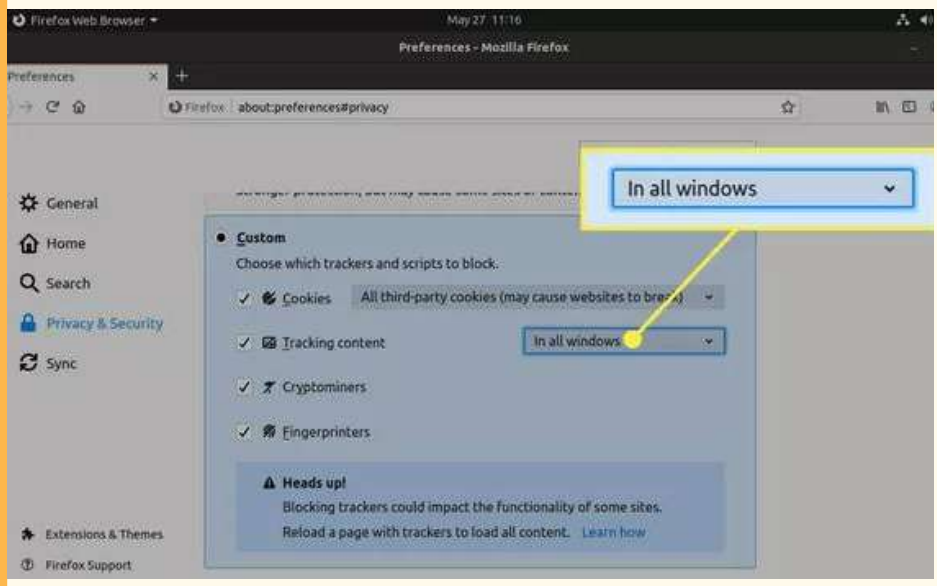
MOZILLA FIREFOX



This browser is set to standard protection by default but for better protection it is important to:

Block 3rd Party Cookies





Follow:

Main menu-> Preferences-> Privacy and Security-> Scroll to 'custom'-> Cookies-> Choose 'All third party cookies'-> select 'Tracking Content'-> Choose 'In all windows'.

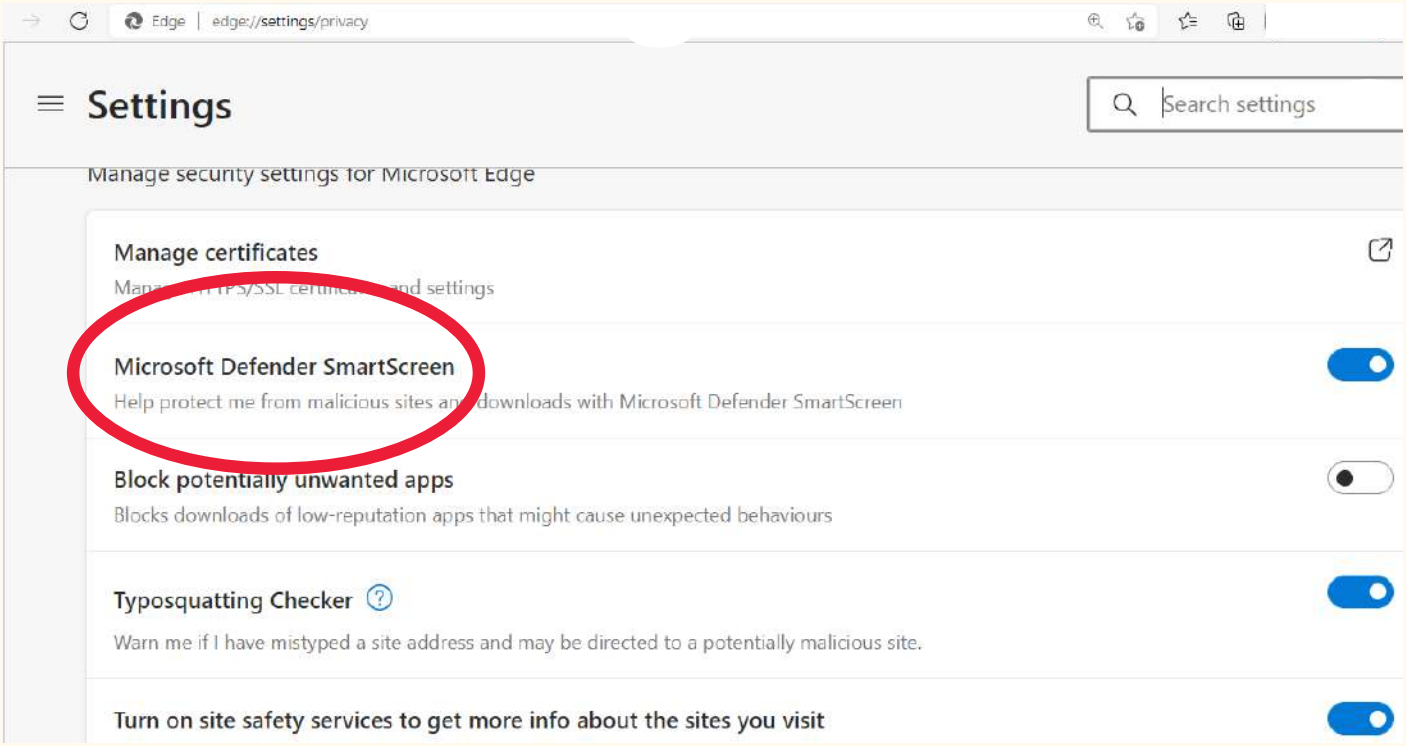
Firefox offers extremely safe browsing experience because of it's wide range of privacy and security features. It includes Security indicators and Malware protection. It helps you to keep your personal information private and control what you share online.

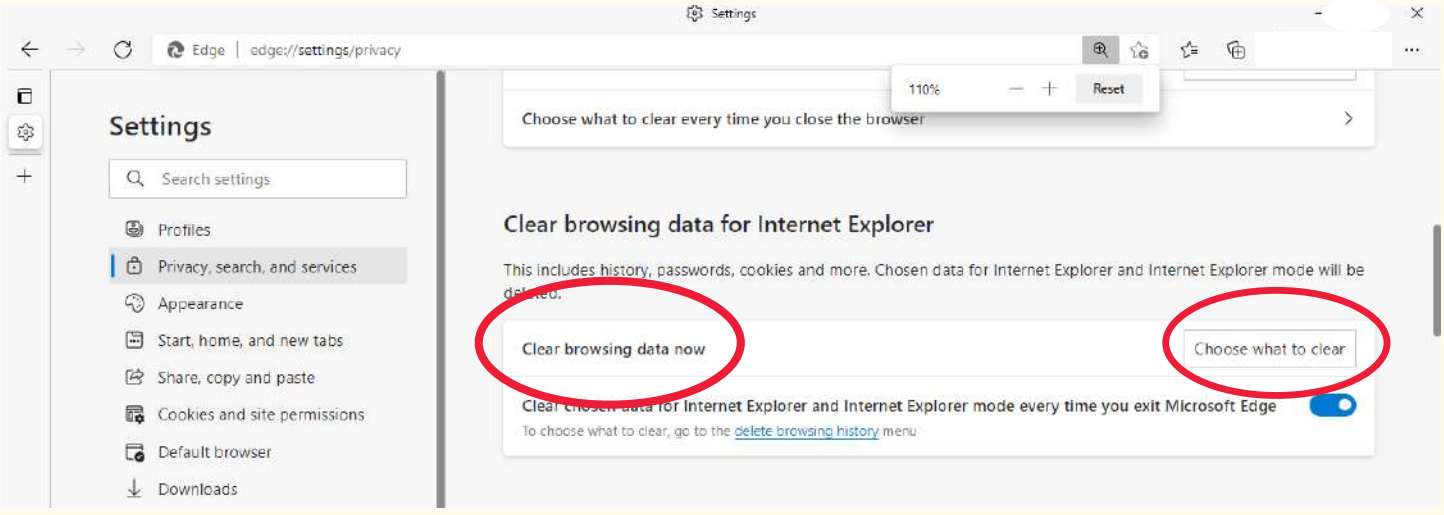
MICROSOFT EDGE

This browser is inbuilt in all Microsoft computers and laptops.

Click ellipses (...)-> Settings and follow:

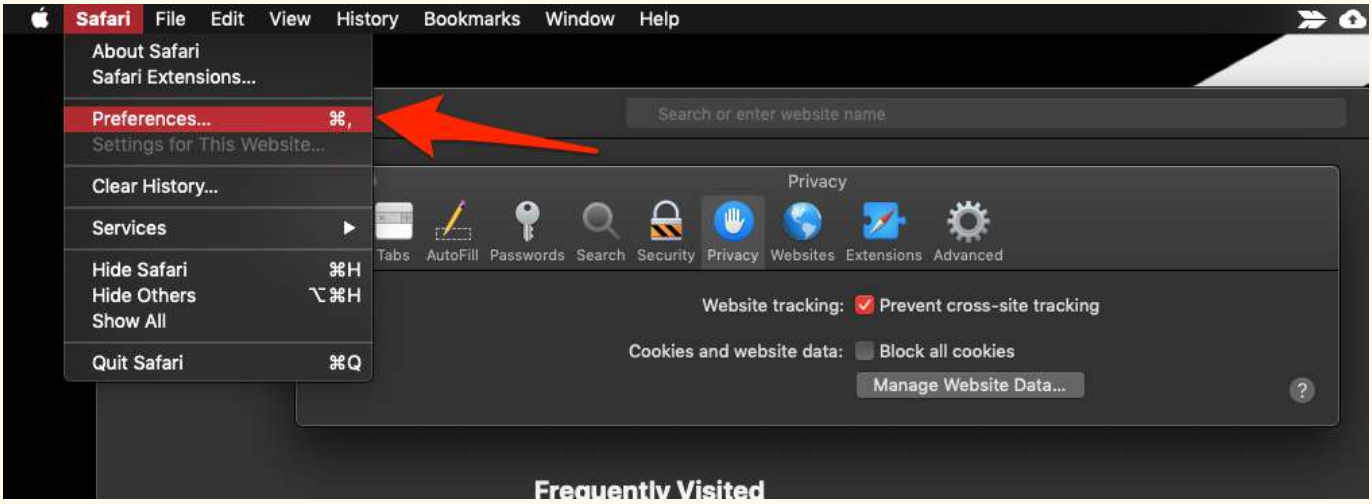
Privacy: Against Clear Browsing Data now and choose 'What to clear.'
Enable Microsoft Defender Smart Screen.
Use Balanced mode but Strict mode is helpful too.
Send Do Not Track Requests; Click to turn on/off.



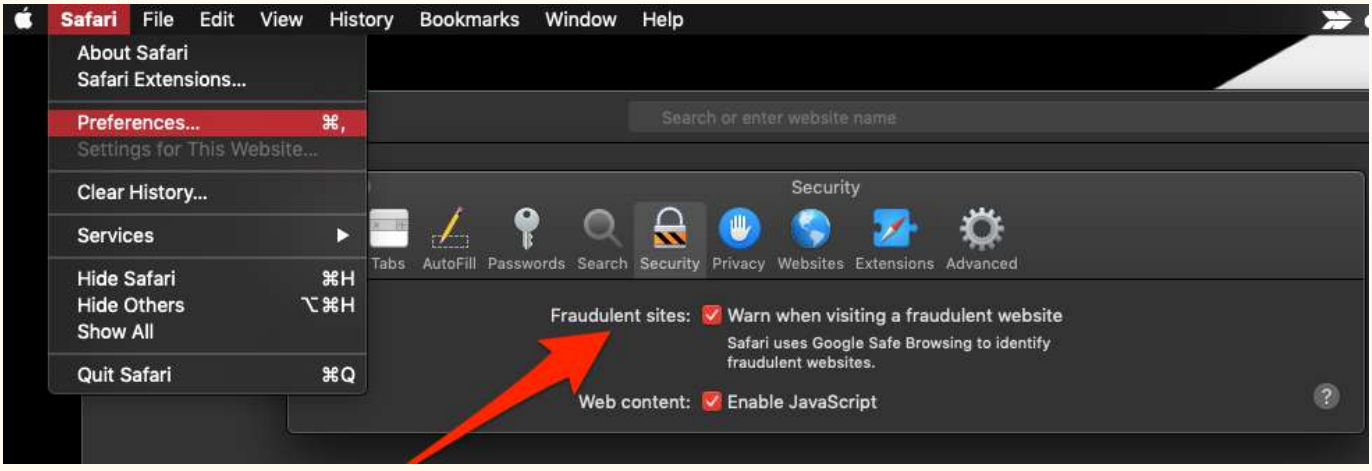


SAFARI (FOR MAC)

After a range of browsers that are compatible with almost all the operating systems, let's come to the inbuilt browser of iOS.



Stop Website Tracking: From menu bar-> Safari-> Preferences-> Privacy tab-> enable checkbox saying 'Website Tracking — prevent cross-site tracking.'

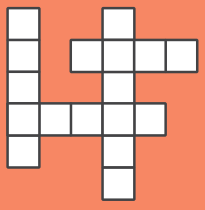


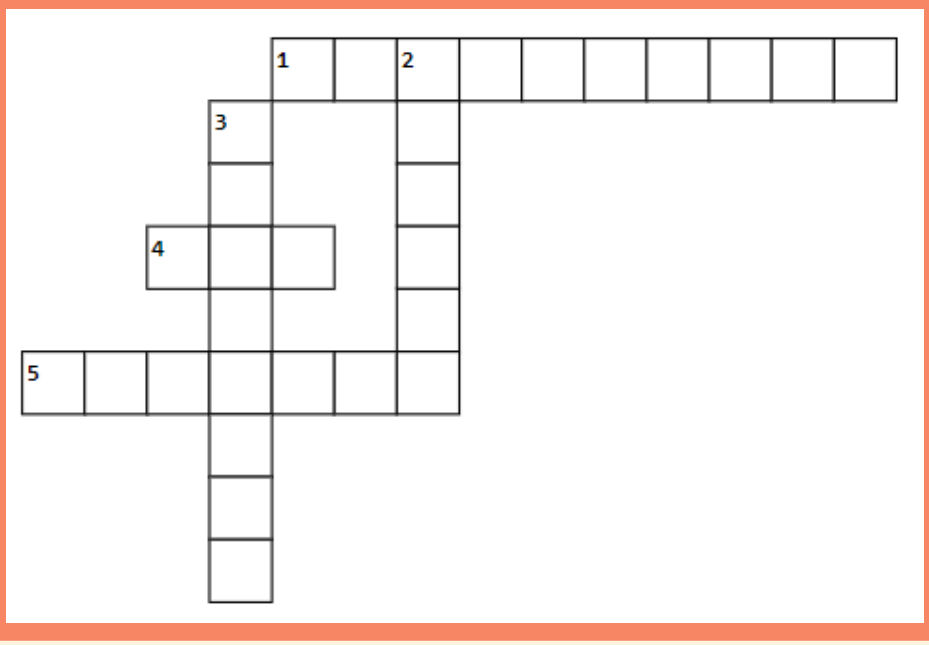
Security from Fraudulent Sites: From menu bar-> Safari-> Preferences-> Security tab-> enable checkbox in front of 'Fraudulent Sites.'

CREDITS

1. WWW.VMWARE.COM
2. WWW.KASPERSKY.CO.IN
3. WWW.PALOALTONETWORKS.COM
4. WWW.ALLCONNECT.COM
5. WWW.INFOSECAWARENESS.IN
6. WWW.WIRED.COM

CROSSWORD TIME!





ACROSS

1. The process of encoding information that converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information.

4. This is a unique identifier used to locate a resource on the Internet. It is also referred to as a web address.

5. Term given to a category of software which aims to steal personal or organisational information. It is used to record the keystrokes which could be fatal as it can record passwords, credit card information etc.

DOWN

2. This is a small file that websites send to your device which is used by the sites to monitor you and remember certain information about you.

3. This is a network security device(hardware or software or both) that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

1. Encryption 2. Cookie 3. Firewall 4. URL 5. Spyware