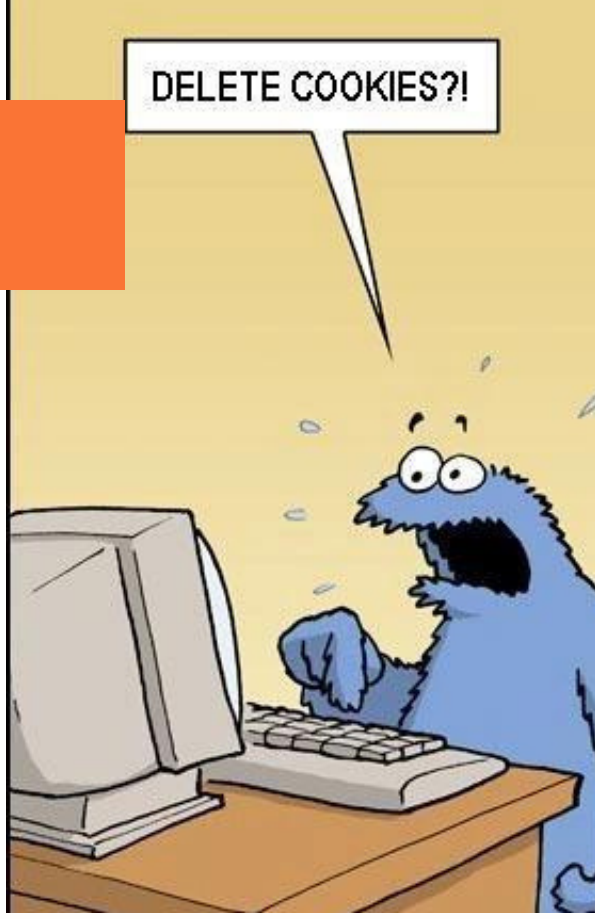
Security Matters

NEWSLETTER



KILL THE COOKIES. SHIELD YOUR INTERNET HISTORY

Your browser has a lot of your information stored including the websites you visit, your passwords, browsing history, data you have downloaded, and more. You might have seen cookies pop-ups asking you to accept cookies when you visit websites. These cookies are files created by websites that you visit and stored on browsers. It can be used to track any kind of data about you such as search and browsing history, IP address, on-site behavior like scrolling speed, etc.

The browser cache remembers parts of pages, like images, to help the browser load a webpage faster during your next visit. If you surf the web frequently and visit a variety of websites, the cache can take over a lot of the storage space on your device.

HOW TO CLEAR COOKIES?

Safari

Safari > Preferences / Settings > Privacy > Manage website data / History > Clear history and data > Select a timeframe for how far back you want to erase

* This step is deleting the browser history, takes out cookies and cache as well.

Google Chrome

Google Chrome > Menu icon (Three-dot in the top-right corner) > Settings > Privacy > History > Clear browsing data > Cookies & other site data > Clear cache / clear data

Mozilla Firefox

Mozilla Firefox > Menu icon (Three-dot in the top-right corner) > Options / Preferences > Privacy & security > Cookies and site data > Check the option and Clear data > Clear

Microsoft Edge

Microsoft Edge > Menu icon (Three-dot in the top-right corner) > Settings > Privacy, search and services > Clear browsing data > Choose what to clear > Cookies and other site data > Clear

HOW TO CLEAR CACHE?

Settings > **Safari** / specific app to clear cache > History > Clear history and website data / Clear cache > Confirm

Settings > Apps / Application manager > Choose any specific app to clear cache > Look for "Storage", "Apps" or "Storage & cache" > Clear cache

HOW TO TURN OFF LOCATION TRACKING?

Location data is incredibly revealing of a person's life. Tech companies use the location services on your smartphone to track your comings and goings. That's how they give you up-to-date traffic and weather reports, restaurant recommendations, and other information. But they may also sell that information to marketers and others interested in studying your habits. You can't completely stop your smartphone from providing clues about where you go, but you can do a lot to reduce the data collection and make it less precise.

Apple

Settings > Privacy > Location services > Choose an app > Choose either "Never", "Ask me next time" or "While using the app"

Google

Google account > Menu > Data and personalization > My activity > Location services >Disable the switch off button

Samsung

Settings > Apps > Permission manager > Location > Turn off the location permission

Xiaomi

Settings > Privacy / Privacy and security > Location > Choose an app > Turn off the location permission

Huawei

Settings > Apps & notification > Permissions > Location services > Choose an app > Disable location access / Choose your desired option

Realme

Settings > Privacy > Location services > Disable location access / Choose your desired option

Oppo

Settings > Privacy > Apps > Permissions > Location > Disable location access / Choose your desired option

Vivo

Settings > Location > App location permissions / Location services > Disable location access / Choose your desired option

Facebook > menu icon (on Android, three-dot at the top right) (on iOS, three-dot at bottom-right) > Settings & privacy > Settings > Location > Location services > Disable location access

TikTok > Profile icon (bottom-right corner) > menu icon (three-dot at the top right) > Privacy and safety > Personalization and data > Disable the option for "Location services"

Twitter > Profile icon (top-left corner) > Settings and privacy > Privacy and safety > Select "Precise location" > Disable the option to stop sharing your location

Instagram > Profile icon (bottom-right corner) > menu icon (three-dot at the top right) > Settings > Privacy > Select Location > Disable location access

LinkedIn > Profile > Settings > Privacy > Location services > Choose your desired location settings

YouTube > Profile picture / menu icon (three-dot at the top right) > Settings > General > Location settings > Choose your desired location settings

*Please note that all the instructions above are general and may vary slightly depending on the version of the app or your device's operating system or browser platform.

Related News

Seized Swatch watches have LGBTQ inscriptions

It is claimed that raids conducted by the Ministry of Home Affairs (KDN) on Swatch stores across the nation a couple of weeks prior only confiscated specific models, an alleged ministry insider claims.The source revealed that the timepieces targeted are only those that contain the letters "LGBTQ" inscribed on the face, which stands for "Lesbian, Gay, Bisexual, Transgender and Queer."
Read more: https://bit.ly/3fMmmFI

Watch out: fake Meta message on Instagram, trying to steal passwords

Instagram users are being warned to watch out for a fake direct message accusing them of copyright infringement on their Instagram page and seeking to steal passwords through a pretend appeal form.
Read more: https://bit.ly/3VH2UuF

WhatsApp can now silence unknown callers

WhatsApp has added a new update to give users the option to mute calls from unknown numbers. The company explained that the 'Silence Unknown Callers' update helps to give users more privacy and control over incoming calls.
Read more: https://bit.ly/467213E

Over 100k+ compromised ChatGPT accounts on dark web marketplaces

These hacked credentials were found in the logs of information-stealing malware sold on illegal dark web markets. Info stealers are a sort of malware that gathers information from installed browsers on infected machines, including cookies, browsing history, bank card information, credentials saved in browsers, and other information, before sending it all to the malware operator.
Read more: https://bit.ly/3yvMhs0

MCMC to take legal action against Meta over malicious content on Facebook

The Malaysian Communications and Multimedia Commission (MCMC) has announced that it will be taking definitive steps or legal action against Meta as the social media platform has failed to take sufficient action to address Facebook scam ads, impersonation, online gambling and undesirable content related to Race, Royalty and Religion. This comes after increasing public concern and Meta's response has been sluggish and unsatisfactory.
Read more: https://bit.ly/3EAcSrq

Related News

UNESCO proposal hurts democracy and the internet by encouraging administrative online censorship in Asia

UNESCO's proposal to encourage administrative online censorship in Asia is a problem. It could lead to governments controlling the internet and limiting the information people can share. This goes against democracy and freedom of speech. Instead, UNESCO should focus on tackling disinformation and hate speech without supporting censorship.
Read more: https://bit.ly/3fMmmFI

DuckDuckGo browser beta for Windows bakes in a lot of privacy tools

Privacy-focused firm DuckDuckGo has released a public beta of its browser for Windows, offering more default privacy protections and an assortment of Duck-made browsing tools. However, it has no extensions yet, but it can fight spam, tracking, and YouTube's algorithm.
Read more: https://bit.ly/3JI4Cr9

Malaysia warns people against downloading malicious 'Pink WhatsApp'

The Commission said the application is being falsely advertised with claims that it has better security and privacy offerings, along with other features like a customised interface and the ability to send larger files compared to the popular WhatsApp application by Meta. However, MCMC said the app poses a security risk as it can access certain items on the user's device such as photos, contacts list and SMS.
Read more: https://bit.ly/467213E

Instagram and Messenger get more parental supervision tools

Meta is releasing additional tools for parents and guardians who want to know more about how their children are interacting with apps like Instagram, Messenger, and Facebook. One of the new features offers parents to view the amount of time their teen is spending on Messenger and the information on their teen's message settings.
Read more: https://bit.ly/3yvMhs0