SECURITY MATTERS
NEWSLETTER

WATCH WHAT YOU SAY & DO!
WE KNOW WHO YOU ARE..

VOL 3 • AUGUST 2022

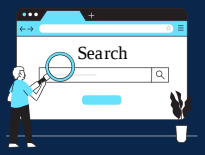
With the Pegasus spyware abuse emerges in Thailand, and the new DNS.id plan which will create a more centralized censorship system through a unified national DNS in Indonesia, it's becoming more and more obvious that Internet regulations and censorship are becoming the norm. Nobody wants to use the internet with someone constantly looking over their shoulder, everyone want to use the internet freely and openly without worry.

Internet surveillance refers to your computer and online activity, data and Internet traffic being monitored and logged by government agencies, Internet Service Provider (ISPs), private companies, and hackers. It allows respected party to gain deep understanding of a target and often as an enabler of censorship. Basically, every step you take in the virtual world is carefully watched, recorded and then used for one purpose or another.

Who is watching you?

For national security reasons, as they claimed to collect data on potential criminals, and to prevent terrorist acts.

Know everything about your browsing habits and these information can be passed on to surveillance agencies; sell user's data to third-party advertisers for profits; might engage in bandwidth throttling (intentionally slowing speeds) if they notice you're using 'too much data' for various online activities.



Most tracking done through cookies which help with loading preferred contents to improve user experience, selling to advertisers to build accurate profiles of online users that are used to set up targets ads.

Most tracking done through cookies which help with loading preferred contents, selling to advertisers to build accurate profiles of online users that are used to set up targets ads.

Stealing your identity, blackmail and sell your personal data scammers, etc.

General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me

More information about Security Matters, visit www.securitymatters.asia
info@securitymatters.asia
@secm8 @sec_matters

SECURITY MATTERS
NEWSLETTER

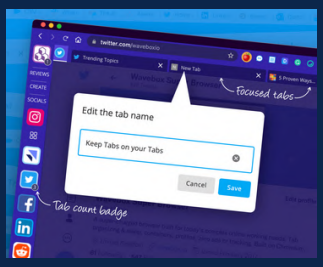
WATCH WHAT YOU SAY & DO!
WE KNOW WHO YOU ARE..

VOL 3 • AUGUST 2022

How do they tracking on you?

Browser fingerprint
Stitches together information about your device to create a unique intensifier's that used to create all of your online activity

Cookies
Collect information on how you interact with website



Account tracking
Keep tabs on your online activity while logged into an online account/platform

Web beacons/bugs
Track how you engage with a webpage, including the content you click

DNS poisoning/spoofing
Hackers redirect web traffic toward fake web servers and phishing websites to trick you into sharing sensitive information

Location tracking through WiFi or GPS

General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me

More information about Security Matters, visit www.securitymatters.asia
info@securitymatters.asia
@secm8 @sec_matters

SECURITY MATTERS
NEWSLETTER

WATCH WHAT YOU SAY & DO! WE KNOW WHO YOU ARE..

VOL 3 • AUGUST 2022

What can I do about it?

Here are some ways to make it harder to track your activity and mitigate the threat of online surveillance:

Use a private browser (i.e. Tor browser, Firefox) and search engine (i.e. DuckDuckGo) to minimize covert data sharing

Use protection tools like VPN (i.e. ProtonVPN, TunnelBear, Express VPN)

Update browser settings and use browser plugin to prevent tracking and block third-party cookies/pop-ups. (i.e uBlock Origin)

Use an Ad blocker (i.e. AdGuard)

Only visit HTTPS sites

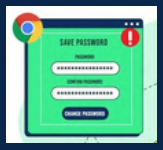
Encrypt your online and offline data

Enable automatic updates

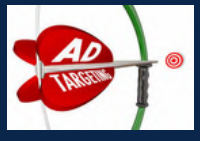
Be aware of phishing attacks. Think before you click.

Do not allow cookie tracking on website

Use two-factor authentication (2FA) or multi-factor authentication (MFA)



Switch off password auto-save in the browser



Opt out of targeting advertising and data broker sites in social media (i.e. Facebook)

Avoid adverts disguised as fake download links

Even if you have nothing to hide, you still have the right to privacy, and you need to protect it. So stay updated at all times, and always practice good habits to secure your personal information to avoid Internet surveillance.

SECURITY MATTERS

General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me

More information about Security Matters, visit www.securitymatters.asia
info@securitymatters.asia
@secm8 @sec_matters

Related News

Tor browser now attempts to bypass internet censorship automatically

The latest version of Tor is available for download on the Tor Project website and it will significantly improve the user experience of connecting to Tor from heavily censored areas. In the new version, users no longer have to manually try out bridge configurations to unblock Tor.
Read more: https://bit.ly/3PIX1bW

Malaysia among least cyber-secure countries worldwide — data

Malaysia, Indonesia and Thailand has been ranked among the top 10 Asian countries that are the least secure to work remotely. This research analysed the cyber threat landscape within each country considering the prevalence of phishing and malware along with botnet networks.
Read more: https://bit.ly/3BFraWs

Facebook takes down massive internet 'troll farm' in Malaysia allegedly linked to PDRM

The Royal Malaysia Police (PDRM) has been linked to a troll farm that promotes the government and criticises its detractors, according to a report by tech giant Meta. Meta, in its Quarterly Adversarial Threat Report, claimed that 596 Facebook accounts, 180 pages, 11 groups and 72 Instagram accounts in Malaysia were removed for violating the policy the platforms' policy against coordinated inauthentic behaviour.
Read more: https://bit.ly/3bup6pJ

iPay88 reports system breach. User card data may be compromised

Local online payment gateway iPay88 believes that user personal data in the form of card information may have been compromised by attackers. This is undeniably worrying, as a large number of local online stores, e-wallets, credit cards, Buy Now Pay Later (BNPL) services, and banks rely on its online payment gateway.
Read more: https://bit.ly/3Py3Q0h

As spyware abuse emerges in Thailand, the pressure for accountability mounts across the world

Last month, a report by Thai civil society groups revealed that the devices of at least 30 people in Thailand had been infected with Pegasus. Barely five days after the report was released, five members of Thailand's political opposition revealed their devices had also been compromised. Across the globe, revelations are emerging of governments using invasive technology to track, target, and silence critics.
Read more: https://bit.ly/3CreHpG

SECURITY MATTERS
General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me

More information about Security Matters, visit www.securitymatters.asia
info@securitymatters.asia
@secm8 @sec_matters

Related News

Twitter informs users of data breach which exposes emails and phone numbers of pseudonymous accounts

Twitter has sent out emails to users who are affected by a security vulnerability. Apparently, the issue was discovered in January this year and it was reported that phone numbers and email addresses belonging to 5.4 million accounts have been stolen and put on sale.
Read more: https://bit.ly/3vXOHhA

Google Chrome Patches Multiple Security Bugs

Google said Tuesday that it patched multiple security bugs in Chrome, adding that one bug is being actively exploited. Because of this threat, Chrome users should update their browser as soon as possible.
Read more: https://cnet.co/3CpJq6C

How Lese Majeste Law are eroding free speech in Southeast Asia

Lese Majeste, the crime of insulting the monarchy, is an outdated defamation offense that provides extra protections to unelected rulers. Across Southeast Asia, increasingly authoritarian governments are systematically corroding freedom of expression as their tolerance for dissent and criticism deteriorates. States continue to harass, sue, and imprison activists and human rights defenders at alarming rates.
Read more: https://bit.ly/3AiH3Qj

Your iPhone/iPad may have been leaking data all along while using a VPN on it

Many people use VPN to increase the privacy and security of their Internet browsing, as well as to access content outside of their region. For most people, this means you get a completely secure connection with no ability for corporations or governments to spy on you – but that's apparently not the case for iOS users.
Read more: https://bit.ly/3c8GfWl

Cybercriminals Using Google Ads To Scam Victims

Cybercriminals are coming up with a new ingenious tactic of hooking victims, which is by using Google's own advertising system. Whenever you type in, for example, YouTube in a browser search bar, Google will more often than not put an ad for the YouTube home page at the very top of the search results.
Read more: https://bit.ly/3PTgsil

SECURITY MATTERS

General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me

More information about Security Matters, visit www.securitymatters.asia
info@securitymatters.asia
@secm8 @sec_matters