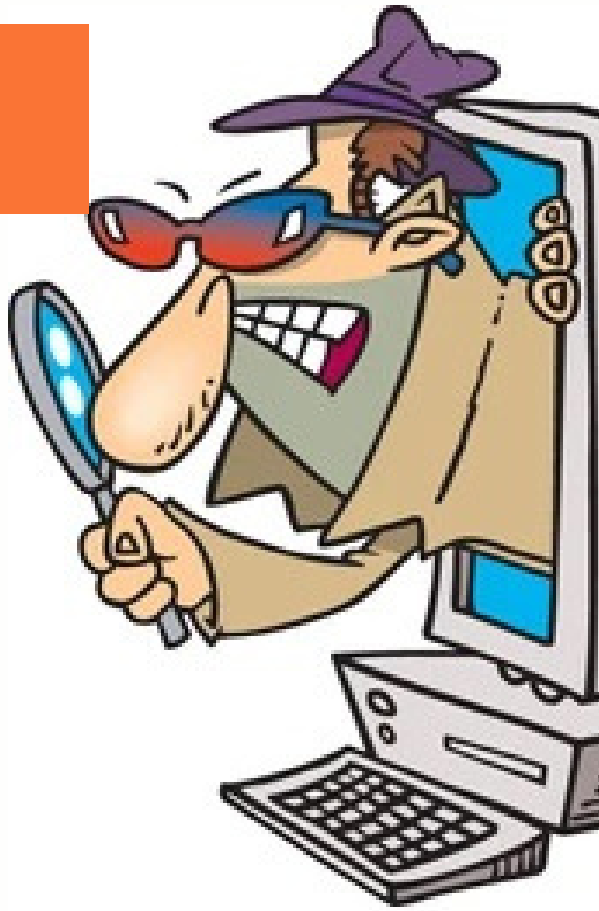
Security Matters

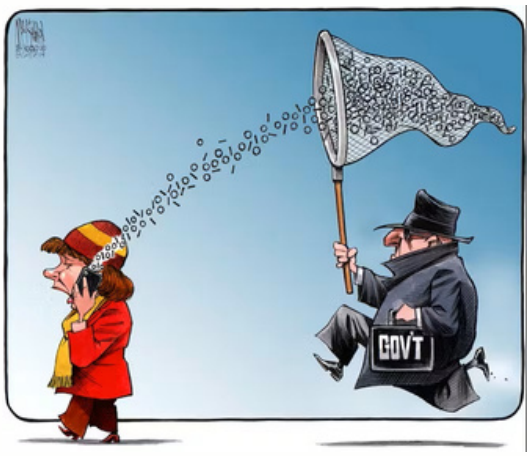
NEWSLETTER



THE CYBERSECURITY'S CREEPIEST THREATS

Surveillance software like spyware or stalkerware is becoming more advanced nowadays. It can be used by hackers to monitor or track the activities of individuals without their consent. No one should snoop on your phone or laptop, be it your boss, partner or even the authority.

Spyware is generally more well-known than stalkerware. You could unknowingly infect your device with malware by downloading a malicious file/app. Spyware can also be spread to a device via phishing attacks. Once spyware has infected a device, it can put a person's data and safety at risk. The recent example, Pegasus, a government-grade commercial spyware which sold as a tool to governments for combating terrorism and for law enforcement purposes, allows governments to hack a phone and steal the data of the targeted.



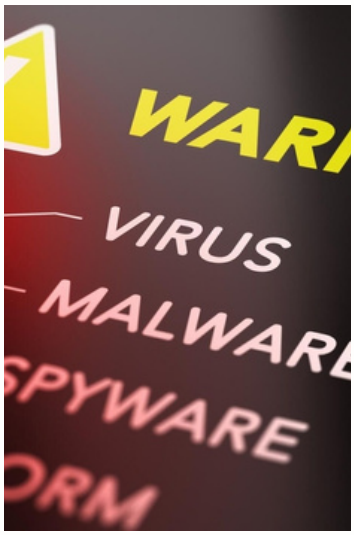
However, stalkerware is a more personal way of invading someone's privacy because it has to have direct access to the victim's devices they're trying to infiltrate. Therefore, stalkerware is generally used by someone who knows the victim like a parent or partner.

SIGNS OF SPYWARE/STALKERWARE ATTEMPTS

- Battery drains faster than ususal
- Device is overheating or feels warm even when not in use and not charging
- Mobile data usage increases drastically
- Longer shutdown time / response times than usual
- Clicking, static, echo-y, or distant voices can be heard when on a call

Certain app permissions enable/disable without your consent	Location and Bluetooth are turn on automatically	Unexpected reboot or shutdown	Changes in settings without your knowledge	Slow performance. Unusual processes running in your app managers.
Unusual text messages or emails or notifications	Your device turns on Wi-Fi or mobile internet even though you turned them off	Your device light up when in standby mode	Your device behaving strangely after leaving it unattended	Increase in unwanted pop-ups or ads

HOW TO PREVENT?



- Install antivirus and anti-malware software. E.g. Windows Security, Malwarebytes, Avast
- Update Operating system and software regularly.
- Always check the app's permission list before downloading an app. Restrict or deny access to functions that are not needed for the app to work.
- Beware of phishing attacks, unknown sources and unusual behavior on your device (as mentioned above)
- Secure your devices against all unauthorized physical and online access. Set up passwords, two-factor authentication (2FA) and encrypt your devices.
- Use a Virtual Private Network (VPN). E.g. Proton VPN, Express VPN, TunnelBear
- Never install apps from unknown sites. Always download from trusted sources. E.g. Google Play Store, Apple Store
- Use an alternative browser like Firefox instead of default Safari or Chrome.
- Review installed apps and check app permissions regularly.

HOW TO REMOVE?

Spyware and stalkerware are hard to detect and can be just as hard to remove. It is not impossible in most cases, but it may take some drastic steps on your part. Sometimes the only option may be to abandon your device. Do not tamper with your device if you feel your physical safety may be in danger. Instead, reach out to the police and supporting agencies.

- Remove suspicious apps.
- Run an anti-malware & antivirus scan.
- Disable location tracking.
- Update Operating system.
- Change passwords in critical accounts immediately and enable 2FA
- Reboot your device.
- Enable app installation from trusted sources only.
- Revoke app permissions. Check here: "How to check app permissions in my mobile device?"
- Check if any suspicious browser extensions and remove them immediately.

If all the above fails, perform a factory reset.
On **iOS**, Settings > General > Transfer or Reset phone.
On **Android**, Settings > General Management > Reset > Factory Data Reset
*Before factory reset, remember to backup your data.

*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.

Note

Removing spyware and stalkerware can be a challenging task, especially for more advanced variants. If you are unsure about how to proceed or if you suspect that you are a victim, seek help from a professional or contact law enforcement for further assistance. Additionally, if you believe you are a victim of stalking or harassment, report it to the appropriate authorities. It is also recommended that individuals who suspect a Pegasus infection make use of a secondary device for secure communication.

Related News

Android GravityRAT spyware steals WhatsApp backup files

A recently discovered Android virus named "GravityRAT" has rapidly circulated through a new Android malware campaign. It gains access to phones by disguising itself as a fraudulent chat app called 'BingeChat' in order to steal users' sensitive data.
Read more: https://bit.ly/44Gq2gO

New phishing attack spoofs Microsoft 365 authentication system

A provider of email security and threat detection services has recently discovered phishing attack that involves the spoofing of the Microsoft 365 authentication system. The attack begins when the victim receives an email containing a malicious HTML file as an attachment. When the victim opens the file, a phishing page masquerading as Microsoft 365 is launched in their web browser.
Read more: https://bit.ly/3VH2UuF

Two spyware apps on Google Play with 1.5 million users sending data to China

Two file management apps on the Google Play Store have been discovered to be spyware. Both spyware apps, namely File Recovery and Data Recovery (com.spot.music.filedate), and File Manager (com.file.box.master.gkd) are seemingly harmless Android apps use similar malicious tactics and automatically launch when the device reboots without user input.
Read more: https://bit.ly/3NRg991

WhatsApp to let you hide your phone number in communities

Currently, the community participants list is already hidden in the community announcement group but if a user interacts with messages using reactions, the user's phone number would be revealed. The new phone number privacy feature on WhatsApp will ensure that your info stays hidden even with message interactions.
Read more: https://bit.ly/3yvMhs0

Beware of Big Head ransomware: spreading through fake Windows updates

A developing piece of ransomware called Big Head is being distributed as part of a malvertising campaign that takes the form of bogus Microsoft Windows updates and Word installers. Big Head has its ability to function as a data wiper. If the victim fails to pay the ransom in a timely manner or refuses to comply, the ransomware will execute the wiping of data, and also possesses the capability to infect backup systems and archives that are connected to the same network.
Read more: https://bit.ly/3OcaAmQ

Clever Letscall vishing malware targets Android phones

A sophisticated voice-based phishing malware is targeting Android handsets and bilking private financial data from targets, part of a trend raking in millions of dollars of profits using vishing attack techniques. Unlike typical and simple vishing scams, these attacks hijack handsets, implants pre-recorded voice messages and re-routs calls to scammer call centers.
Read more: https://bit.ly/3yvMhs0

Bangkok Post among 300 victims if ransomware attack

The Bangkok Post website was inaccessible for most of Wednesday, along with the sites of hundreds of other internet service users, due to a rare ransomware attack, according to its long-standing service. Bangkok Post readers had no access to the website, and staff were unable to update the contents, from early Wednesday morning until shortly after 7.30pm.
Read more: https://bit.ly/3EAcSrq

Scam alert: How oversharing leaves you vulnerable

A recent survey by Southeast Asian market research and data analytics firm Milieu Insight involving 2,500 respondents in five countries, including Malaysia, found that the most common scams Malaysians fall victim to are buying and selling scams, investment scams and phishing spams. “The thought of ‘it will not happen to me’ is one of the greatest challenges. We often underestimate the risk of falling victim to scams,” said by a representative at Milieu Insight.
Read more: https://bit.ly/44fp8Y6

These Samsung phone flaws have been exploited by spyware

The US Cybersecurity and Infrastructure Security Agency (CISA) has warned that flaws in several Samsung mobile devices have likely already been exploited to by a spyware vendor. They may be old flaws, but they're still being exploited.
Read more: https://bit.ly/3yvMhs0

Proton VPN maps usage to resist censorship - how Proton is defending digital freedoms

VPNs play a crucial role in enabling people to exercise their right to freedom of information and freedom of speech. Popular cybersecurity company Proton has launched a new site to monitor those usage spikes to act as an alarm bell when sudden censorship takes place.
Read more: https://bit.ly/3JU2ugb

Malvertising attacks drops BlackCat ransomware via fake search results

Happeneing through Google Search, hackers use a malicious ISO archive to distribute files that direct users to fake download pages of popular business applications. These apps include AnyDesk, AnyConnect, WinSCP, Treesize, Cisco, Slack, and more.
Read more: https://bit.ly/3JU2ugb