MERCOLA
Take Control of Your Health

TikTok Caught Tracking Keystrokes, Including Passwords

Analysis by Dr. Joseph Mercola ✔ Fact Checked | October 19, 2022

STORY AT-A-GLANCE

- Apps such as Instagram, TikTok and Facebook inject JavaScript code into third party websites that cause potential security and privacy risks to the user
- Without your consent, when you click on a link to an external website from an app, code may be inserted that allows the app to monitor every button or link you tap, text you select, screenshots you take and anything you input into the site
- When comparing several iOS apps, including Amazon, Facebook Messenger and Robinhood, only TikTok neglected to offer users an option to switch from in-app browsing to using an external browser when viewing third-party sites
- TikTok's parent company is ByteDance, which has ties to the Chinese Communist party, which means the app's surveillance capabilities could potentially be used for industrial espionage purposes
- No matter what app you're using, you should assume that someone, or some entity, may be watching you

You may assume your privacy is at risk when you give out information online, but even just browsing could pose a security risk, according to software engineer and security researcher Felix Krause.[1]

This is particularly true when you're scrolling through an app on your cellphone, as in-app browsers may be monitoring virtually everything you're doing, including your keystrokes, giving away credit card information, passwords and other sensitive data.

In-app browsing occurs when you browse third-party sites that open in the app as opposed to a separate browser. Krause found that in-app browsing initiated in the TikTok app includes a Java Script code that allows the social media giant to follow every screen tap and text input.

Are Social Media Apps Logging Your Keystrokes?

Krause, founder of Fastlane, an open source tool for iOS and Android developers, released a report in August 2022 warning of the risks of mobile apps using in-app browsers. In particular, he wrote, Instagram and Facebook apps "inject JavaScript code into third party websites that cause potential security and privacy risks to the user."[2] Krause explains:[3]

> *"The iOS Instagram and Facebook app render all third party links and ads within their app using a custom in-app browser. This causes various risks for the user, with the host app being able to track every single interaction with external websites, from all form inputs like passwords and addresses, to every single tap."*

What this means is that, without your consent, when you click on a link to an external website from, for instance, the Instagram app, Instagram injects a JavaScript code that allows them to monitor every button or link you tap, text you select, screenshots you take and anything you input into the site. This also occurs if you click on an advertisement in the app.[4] According to Krause:[5]

> *"With 1 billion active Instagram users, the amount of data Instagram can collect by injecting the tracking code into every third party website opened from the Instagram & Facebook app is a staggering amount. With web browsers and iOS adding more and more privacy controls into the user's hands, it becomes clear why Instagram is interested in monitoring all web traffic of external websites."*

In an updated report, Krause also warns that TikTok is monitoring all keyboard inputs and taps from their app:[6]

"When you open any link on the TikTok iOS app, it's opened inside their in-app browser. While you are interacting with the website, TikTok subscribes to all keyboard inputs (including passwords, credit card information, etc.) and every tap on the screen, like which buttons and links you click.

TikTok iOS subscribes to every keystroke (text inputs) happening on third party websites rendered inside the TikTok app. This can include passwords, credit card information and other sensitive user data ... We can't know what TikTok uses the subscription for, but from a technical perspective, this is the equivalent of installing a keylogger on third party websites.

TikTok iOS subscribes to every tap on any button, link, image or other component on websites rendered inside the TikTok app. TikTok iOS uses a JavaScript function to get details about the element the user clicked on, like an image."

'A Huge Risk to Every User'

In a response to Forbes, TikTok confirmed that the features to track users do exist in their code, though they denied using them.[7] Krause also points out that just because an app puts the code into external websites, it doesn't mean that it's doing anything malicious with it. "There is no way for us to know the full details on what kind of data each in-app browser collects, or how or if the data is being transferred or used," he says.[8]

Speaking with The Guardian, TikTok again denied any wrongdoing with their invasive JavaScript code, stating, "Contrary to the report's claims, we do not collect keystroke or text inputs through this code, which is solely used for debugging, troubleshooting and performance monitoring."[9]

Still, the simple fact that the code exists is a red flag, and hints at the massive amount of data that could be collected about you every time you browse the web. Krause notes:[10]

> *"Installing a keylogger is obviously a huge thing ... according to TikTok it's disabled at the moment. The problem is they do have the infrastructure and the systems in place to be able to track all these keystrokes ... that on its own is a huge problem. The fact that they have this system already is a huge risk for every user."*

When comparing several iOS apps, including Amazon, Facebook Messenger and Robinhood, only TikTok neglected to offer users an option to switch from in-app browsing to using an external browser when viewing third-party sites. Overall, Uri Gal, professor of business information systems at the University of Sydney, told The Guardian:[11]

> *"TikTok had the most extensive surveillance capabilities. Many people who use the app are unaware of the surveillance conducted about them within [it]. The user base of TikTok is by far younger than Facebook's and Instagram's ... that makes them much more vulnerable."*

Gal also pointed out that TikTok's parent company is ByteDance, which has ties to the Chinese Communist party. This means the app's surveillance capabilities could potentially "gather as much information as possible for industrial espionage purposes, and shaping public opinion that is more toward their interests."[12]

A report from cybersecurity company Internet 2.0 confirmed TikTok's "excessive data collection" and that the app "connects to mainland China-based infrastructure."[13] While Instagram and Facebook are also guilty of collecting data, Gal noted that TikTok also poses a unique national security threat due to its ties to China.

"Their [Instagram and Facebook's] primary motivation is almost purely commercial and financial," he said, "whereas with TikTok, there is a national security element that I don't think is directly present with the others."[14]

Is Facebook Collecting Sensitive Health Data?

A lot is going on behind the scenes when you browse the web, even when you assume you're in a more protected area, such as a hospital website or a password-protected health information portal like MyChart.[15] Facebook, for instance, may be collecting sensitive health data via pixels, which may be installed on websites you visit without your knowledge.

They can collect information about you as you browse the web, even if you don't have a Facebook account. The Meta Pixel is a piece of JavaScript code that developers can add to their website to track visitor activity.[16] According to Meta:[17]

> *"It works by loading a small library of functions which you can use whenever a site visitor takes an action (called an event) that you want to track (called a conversion). Tracked conversions appear in the Ads Manager where they can be used to measure the effectiveness of your ads, to define custom audiences for ad targeting, for dynamic ads campaigns, and to analyze that effectiveness of your website's conversion funnels."*

An investigation by The Markup tested websites from Newsweek's top 100 U.S. hospitals. Facebook's Meta Pixel was found on 33 of the websites, sending Facebook information linked to an IP address, which identifies individual computers and may be traceable back to an individual or household.

The pixel tracks not only the IP address of the computer being used but also what doctors are searched for and search terms added to search boxes or selected from dropdown menus. The Markup reported:[18]

> *"On the website of University Hospitals Cleveland Medical Center, for example, clicking the "Schedule Online" button on a doctor's page prompted the Meta Pixel to send Facebook the text of the button, the doctor's name, and the search term we used to find her: "pregnancy termination."*
>
> *Clicking the "Schedule Online Now" button for a doctor on the website of Froedtert Hospital, in Wisconsin, prompted the Meta Pixel to send Facebook the*

text of the button, the doctor's name, and the condition we selected from a dropdown menu: "Alzheimer's.""

The data you're accessing when using password-protected patient portals may also be sent to Facebook via pixels. The Markup found the Meta Pixel in patient portals from seven health systems, including Edward-Elmhurst Health, FastMed, Novant Health and Community Health Network.

Data being collected included names of medications being taken, descriptions of allergic reactions and upcoming doctor's appointments.[19] Novant Health, which removed the pixel after being contacted by The Markup, stated, "We appreciate you reaching out to us and sharing this information. Our Meta pixel placement is guided by a third party vendor and it has been removed while we continue to look into this matter."[20]

Be Wary of YouTube and TikTok

The lesson to be learned is that no matter what app you're using, you should assume that someone, or some entity, may be watching you. It's important to remember that the internet was built by the government as a tool to spy on citizens. If you're interested in learning more about the little-known beginnings of the internet, I encourage you to read the book "Surveillance Valley: The Secret Military History of the Internet," by Yasha Levine.[21]

Levine, an investigative journalist, reveals that the internet began in the Vietnam era and was used to spy on guerrilla fighters and antiwar protestors, "a military computer networking project that ultimately envisioned the creation of a global system of surveillance and prediction." However, the military surveillance objectives that underpinned the internet's development are still in force today.[22]

The end result, as society becomes increasingly digitalized, is that it's difficult to maintain your privacy online, no matter what website or app you're using. There do, however, appear to be some particularly egregious offenders — TikTok and YouTube among them. Research by URL Genius[23] looked into 200 apps from 20 different

categories, revealing extensive data tracking from most apps, even with very limited app usage.

Further, the tracking may continue on other sites, even after you're no longer using the app.[24] The average number of network contacts per app was six, but this increased to 14 with YouTube and TikTok, although the actual numbers are likely even higher for users who are logged into the apps.

Out of YouTube's trackers, four were from third-party domains — outside parties collecting information and user activities. On TikTok, 13 of the 14 network contacts were from third parties.[25] As noted by URL Genius:[26]

> *"Consumers who have not granted permission to be tracked will be alarmed by the number of 3rd party networks contacted by apps — even with minimal app use. Consumers are currently unable to see what data is shared with 3rd party networks, or how their data will be used ... Consumers do not currently have the ability to disable potential trackers — their options are either use the app or not."*

Krause developed a security tool — InAppBrowser.com[27] — to help reveal what apps are tracking when you're using their in-app browsers,[28] but the safe assumption is, a lot. To take back some of your online privacy, for yourself as well as your children, you can avoid YouTube and TikTok entirely, and try these tips as well:[29]

1. Get rid of Gmail. If you have a Gmail account, try a non-Google email service instead such as **ProtonMail**, an encrypted email service based in Switzerland.
2. Uninstall Google Chrome and use **Brave** browser instead, available for all computers and mobile devices. It blocks ads and protects your privacy.
3. Switch search engines. Try Brave search engine instead.
4. Avoid Android. Google phones and phones that use Android track virtually everything you do and do not protect your privacy. It's possible to de-Google your cellphone by getting an Android phone that doesn't have a Google operating system, but you'll need to find a skilled IT person who can reformat your cellphone's hard drive.

5. Avoid Google Home devices. If you have Google Home smart speakers or the Google Assistant smartphone app, there's a chance people are listening to your requests, and even may be listening when you wouldn't expect.
6. Clear cache and cookies. This will help get rid of invasive computer codes that track what you do online.
7. Use a proxy or VPN (Virtual Private Network). This service creates a buffer between you and the internet, "fooling many of the surveillance companies into thinking you're not really you."

Sources and References

- [1, 10, 28] ABC.net.au August 21, 2022
- [2, 6, 8] Felix Krause August 18, 2022
- [3, 4, 5] Felix Krause August 10, 2022
- [7] Forbes August 18, 2022
- [9, 11, 12, 14] The Guardian August 24, 2022
- [13] Internet 2.0, It's Their Word Against Their Source Code — TikTok Report
- [15, 18, 19, 20] The Markup June 16, 2022
- [16, 17] Meta for Developers, Meta Pixel
- [21, 22] SurveillanceValley.com
- [23] URL Genius January 20, 2022
- [24, 25] CNBC February 8, 2022
- [26] URL Genius January 20, 2022, Why it Matters
- [27] InAppBrowser.com
- [29] Medium March 17, 2017