Vol. 8 | Issue 1

CYBER SECURITY NEWS

January 2023

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter!

Happy New Year! Wishing you and your families a great 2023 with health and blessings. Cheers to another trip around the sun!

1 big thing: ICYMI, Governor Greg Abbott has banned TikTok on state-agency devices

What to know: On December 7, Governor Greg Abbott issued an order to all Texas state agencies banning the use of TikTok, the video-sharing mobile application, on any government-issued devices, including cell phones, laptops, tablets, desktop computers, and other devices capable of internet connectivity.

Read his letter to state agency heads here: https://gov.texas.gov/uploads/files/press/State_Agencies_Letter_1.pdf

Wait, why?: As noted in the letter, it's been found that TikTok collects large amounts of data from users, often taken without the user's explicit knowledge. This data contains sensitive information as well as device brand and model, Operating System (OS) version, mobile carrier, browsing history, app and file names and types, keystroke patterns or rhythms, wireless connections, and geolocation.

Other data collected can include age, image, personal contacts, relationship status, preferences, and other data collected through a single-sign on (SSO) feature that allows users to sign into TikTok from other platforms.

It has also been reported that ByteDance (TikTok's parent company) planned to use location information to surveil individual American citizens and provide its collected data to the Chinese government.

For more details on threats to personal information posed by Tik Tok, please review the following CIS blog post: https://www.cisecurity.org/insights/blog/why-tiktok-is-the-latest-security-threat

Data Privacy

The sheer volume of data generated about you and your activities online is staggering, which is why data privacy has become a defining issue of our digital age. Thousands of businesses across the globe pay top dollar to learn about you through this data.

Your online data can be categorized in certain ways. First, there is personal information like your name, birthdate, and Social Security number. There is also important information about you like your medical records and credit card numbers.

Then there is data about what you do online, like what websites you visit, what products you buy online, and who you communicate with on social media. This data can be extremely granular, like how many seconds you spend looking at a webpage before clicking to something else. Advertisers and other businesses prize this sort of data because they can better target ads and products toward you.

Often, this data is anonymized when sold, meaning an advertiser won't know the specific name of the person who clicked on a link. But a cross-section of data about you can be added together to try to personalize ads to you. (Ever Google something only to see that item pop-up on your social media feed?)

Here are some tips on how to value your data as much as a big tech company does:

- **Know what you can't control.** The truth is you can't control who has access to every scrap and byte of your data. Many online services require some of your data to function – for example, a maps app cannot suggest directions if it doesn't know where you are located (at least while you are using it). Understand that there is a tradeoff between convenience and privacy and make more informed data decisions.
- **Cultivate a data privacy habit.** Apps, websites, devices, and software will often ask to access more data than is necessary. Pay close attention to these requests and actually think about your answers.
- **Check your settings.** Even if an app or software program never asks you for data, you should assume it is still collecting it. Routinely (every month or so) check your privacy settings and ensure everything fits within your comfort level. You can access app and software permissions through your device's general settings.
- **Delete apps you don't use.** Every 3 months or so, go through your devices and think about each app you have downloaded. You might think that the real estate on your phone is limitless, but an app audit isn't just about decluttering. Many apps will collect and share your device-use data even when you don't use them; you're basically giving away your data, and you don't even like the app!

For more information on data privacy: https://staysafeonline.org/programs/data-privacy-week/individuals

In the News

Most apps used in US classrooms share students' personal data with advertisers, researchers find

(Tonya Riley | December 13, 2022)

A whopping 96% of the apps used in U.S. K-12 schools share children's personal information with third parties – including advertisers – often without the knowledge or consent of users or schools, according to a study published Tuesday.

The research, conducted by nonprofit Internet Safety Labs, highlights how the race by schools to increase their tech arsenals has placed students – and parents – in a precarious position of not knowing where personal information is ending up.

Researchers looked at 13 schools in every state, leading to a total of 663 schools representing nearly half a million students. They found that most schools had more than 150 approved technologies for classrooms, a dizzying number for parents and school administrators to monitor. One school had as many as 1,411.

The report follows previous research from the group, formerly known as the Me2B Alliance, finding hundreds of advertisers collected valuable student data from a website specializing in school sports data.

The latest report highlights the exposure of student data to advertisers through school-approved technology is a widespread problem. Nearly a quarter of the apps recommended or required by schools included ads and 13% included retargeting ads, which allow digital advertisers to pinpoint visitors based on previous website visits. Researchers note that this risks student data being pulled into advertising networks without any way for schools or parents to find out. Several states including California ban using student data for this kind of targeting.

The staggering amount of advertising "should alarm everyone," Joel Schwarz, a cybersecurity expert and cofounder of the Student Data Privacy Project, wrote to CyberScoop in an email.

Full Story: https://www.cyberscoop.com/apps-expose-student-data-privacy

A Few More Cyber News Stories:

What You Should Know Before Using the Lensa AI App
https://www.wired.com/story/lensa-ai-magic-avatars-security-tips

Companies spy on your email with invisible images – here's how to stop them
https://bgr.com/tech/companies-spy-on-your-email-with-invisible-images-heres-how-to-stop-them

FBI's Vetted Info Sharing Network 'InfraGard' Hacked
https://krebsonsecurity.com/2022/12/fbis-vetted-info-sharing-network-infragard-hacked

CYBER CHALLENGE

Cyber Sprinters

This Month's Challenge

For this month's challenge, let's play another game!

Cyber Sprinters is a race against the clock to tackle cyber security questions in bid to score points and beat cybervillains.

Granted, this game is geared toward children...ages 7 to 11... so if you want to pass this along to your kiddo to tackle, have at it. Here's your chance to totally dominate, though!

Let me know your High Score. Good luck!

https://www.ncsc.gov.uk/training/ncsc-cyber-security-for-young-people-english-scorm-v2/index.html