Complicated app settings are a threat to user privacy

August 19 2024, by Joseph K. Nwankpa

Credit: Unsplash/CC0 Public Domain

Default privacy settings in popular mobile apps seem like a convenience, allowing you to use a single setting to control the level of privacy—who can see which actions you take—across all of the app's functions. But default privacy settings are also a potential risk to your privacy.

The U.S. app market generated US$44.9 billion in 2023, with smartphone users spending 217 billion hours on their apps. The growing popularity of mobile apps can be attributed to their convenience, ease of use, connectivity and flexibility.

For instance, Venmo, a popular peer-to-peer payment app for iPhone and Android users, lets users send and receive money from anyone with a Venmo account. It is particularly convenient when dealing with transactions that involve multiple people or groups, such as splitting bills.

However, mobile payment apps like Venmo present unique challenges. They combine financial transactions with social media, a blend that can significantly increase privacy risk, especially when coupled with often-ambiguous privacy settings.

Privacy settings complexity

As a cybersecurity scholar, I find that the privacy settings in many apps can often make end users more vulnerable to data exposure despite being presented as enabling privacy. These apps intentionally come with complicated default privacy settings that paradoxically make the user's information more public than private.

Users are often unaware of the additional steps needed for the best privacy settings. Understanding an app's complex privacy policy may require examining the fine print of each app's policy.

For example, Venmo's privacy setting requires the user to choose whether to share transactions or friends lists with the public, only friends, or keep them private. However, users need to set their Default Privacy Settings, Past Transactions and Friends List separately. Default

Privacy Settings do not span all of the app's functions. Also, when you create a Venmo account, all of your transactions are public by default, immediately exposing your financial activities to anyone online.

Unsurprisingly, some high-profile people, including Ohio Sen. and Republican Vice Presidential nominee JD Vance, have left their Venmo privacy settings public, resulting in their Venmo transactions and connections becoming available for anyone using the app to see. These events highlight the importance of understanding these settings to ensure your privacy is protected.

Not just Venmo

But Venmo is not alone in this. Apple released an app called Journal in late December 2023. Journal helps iPhone users write journal entries about their thoughts and feelings. These journal entries can include photos, videos, cities you visited and other personal activities. The app also uses an on-device artificial intelligence feature to provide personalized suggestions on topics relevant to the user.

Users recently discovered that underneath the complicated privacy settings of the Journal app was the "Discoverable by Others" option that posed a serious privacy concern. According to Apple, this feature allows other iPhones that are in your contacts and that have Journal to detect when you are nearby. The purpose is to help prioritize the other users' Journal prompts by including you.

However, the contacts on your phones are not exclusively filled with close acquaintances you are eagerly waiting to discover and have discover you. Instead, your phone contacts may include random numbers such as a plumber you used once for your home maintenance, a realtor who was recommended but you never used, and so on. As with other apps, the concern is that the "Discoverable by Others" feature is the default setting for new users regardless of whether you turned on the journaling suggestions.

How to protect your privacy

The key step to achieving privacy in a world of pervasive digital connections is to take ownership of your data and privacy. As mobile apps continue to access sensitive information about users, it's important to recognize that app providers and owners may not have the incentives to provide the most robust privacy-setting practices. Indeed, failing to effectively manage your app permissions and privacy settings can increase the risk that your data will be exposed to third parties, including people with malicious intent.

Also, too often, users struggle to separate their app contents from their device contents and, in some cases, assume that device-level protections are enough to mitigate the risk of using a mobile app with poor data security protection. But this is not the case. A great rule of thumb is to check each app's default privacy settings after downloading it.

Limiting access rather than granting access is a best practice for privacy. App users tend to incorrectly assume that limiting access can undercut an app's features and quality of service. As a result, when faced with a decision to grant or limit access, people tend to grant access and, in many instances, continue with the default settings.

Staying vigilant

In the era of AI and machine learning technologies, mobile apps can be powerful and provide more personalized services with more data. Still, users should watch out for privacy settings that provide more access and permissions than these apps need to function effectively.

It's important to recognize that the default privacy settings are not always in your best interest. Such settings aim to grant an app access to sensitive data that businesses can exploit and that data breaches can put in the hands of hackers and scammers.

As the complexity of these privacy settings increases, app users need to be aware that protecting their data, now more than ever, requires vigilance.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: Complicated app settings are a threat to user privacy (2024, August 19) retrieved 3 September 2024 from https://techxplore.com/news/2024-08-complicated-app-threat-user-privacy.html