Social Media & Cybersecurity

Office of Information Technology
Division of Information Security
MARCH 2022

There is a saying among cybersecurity professionals that 'Convenience and security are inversely related; the more you have of one, the less you have of the other.' While we may think of this only in terms of access to business or personal email and financial accounts, it also applies to social media. Once only considered a convenient way to stay in touch with friends and family, social media has evolved into a place where users can shop, share information, or even start a business. The proliferation of mobile applications means users can engage in these activities from nearly any location with the touch of a button. This newsletter explores how we should balance such convenience while maintaining security via device control, application settings, and smart social media interactions.

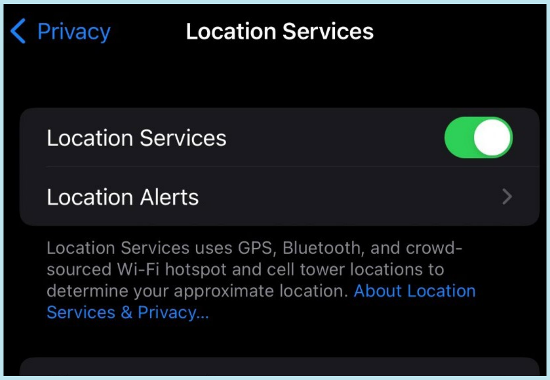
Device Control

Maintaining control of your device is the primary way to keep its information safe. Access to our personal devices often means access to our social media applications as well as the email and financial information connected to them. Limit access to personal devices by using a strong password, passcode, or other authentication methods, like fingerprint or facial recognition. Most devices include an auto-lock feature triggered when the device remains idle for an amount of time you can specify. Once the device locks, the user must authenticate again to gain access.

Maintaining control includes limiting technical access. Rely on trusted sources the device manufacturer manages to install applications and make sure you read application reviews to see if other users have experienced privacy or security issues. Use caution when connecting your personal device to an untrusted wireless network. If you are traveling or teleworking with a government-furnished device, ensure you are using only password-protected Wi-Fi and the IHS Virtual Private Network (VPN) to conduct IHS business. Without knowledge and assurance of a network's settings, you are risking unauthorized observation or capture of your activity.

Application Settings

One of the best ways to secure a social media application is to review and adjust its settings. While one way is to make sure you are using the most recent version, it can also include using application or device settings to control how much information the application can access. When adjusting application settings, think about how much information you want to share with people who can see your profile. For instance, consider whether you want to include location tracking, employment, or relationship status information. While these details establish a means to connect with others with common interests or circumstances, once you have a connection that knows this information, they can share it with anyone. After each application update, review settings to ensure they have not reset to their most permissive state.


< Privacy

Location Services

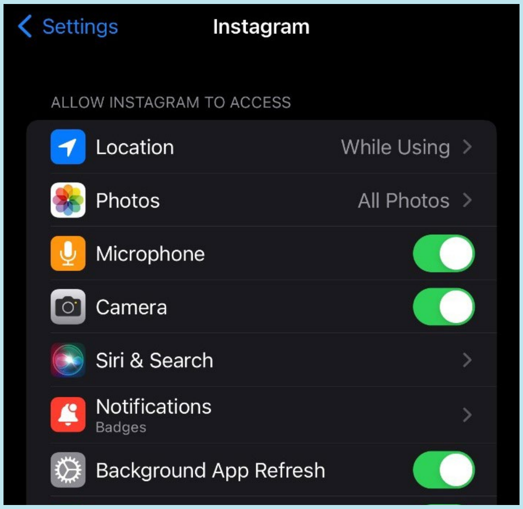
Location Services ●

Location Alerts >

Location Services uses GPS, Bluetooth, and crowd-sourced Wi-Fi hotspot and cell tower locations to determine your approximate location. About Location Services & Privacy...

Figure 1 - Device Location Services Settings

In some cases, you can use your social media credentials to log in to other sites, giving you one less set of credentials to remember, a convenient alternative to memorizing multiple usernames and passwords. On the other hand, using the same set of credentials across sites also means that once a malicious person learns that information, they can access any of those sites and view or use your information. Accessing an account this way connects your social profile with those sites and gives access to your information in accordance with the sites' terms of use. Most people do not read the terms of use and are sharing information about themselves and their social media connections without considering how the information may be used, or who is able to access it. While this is certainly more convenient than remembering a new set of credentials, it is also less secure, so a best practice is to do this sparingly, or not at all.



ALLOW INSTAGRAM TO ACCESS

Location While Using

Photos All Photos

Microphone

Camera

Siri & Search

Notifications
Badges

Background App Refresh

Figure 2 - Social Media Application Settings

Whether a smartphone, laptop, or tablet, all mobile devices allow you to limit what content applications can access. Use the device's privacy and security settings to reinforce social media account security settings. For instance, limit the application's ability to access your camera, microphone, photos, location, or contacts. The most permissive setting for this kind of access grants applications the ability to view content on your device at all times, even if you are not using the application.

Interactions

Every social media connection represents an opportunity for your information to fall into the wrong hands or be used in a way that you do not intend. First, make sure you share personal information with care. For instance, be wary of seemingly innocent questionnaires that ask about your family and their personal details associated with them, like anniversaries, birth dates, and previous residences, or even details about your high school mascots or first car. A malicious person can use this information to predict your passwords, security question responses, or other credentials to gain unauthorized access to any of your accounts.

Also, click with care. Just as in email, malware has found its way to social media environments. Be suspicious of offers that seem too good to be true, or require you to take immediate action to avoid dire consequences. Clicking a bad link can cause the installation of ransomware, viruses, or even key loggers, where the software records every keyboard stroke and sends the information to the attacker.

Conclusion

It is important to balance social media device convenience and security so that we are not sacrificing too much of one to get more of the other. Though it allows us to participate in an increasingly connected world, we should ensure we are connecting and interacting in ways that are safe and sensible. Connect only with people you know and trust, making sure to share information about yourself sparingly. Keep your device secure and manage device connections with care. Feel free to use this information and share it with friends and family.

Please report any agency-related information security incidents to the IHS Cybersecurity Incident Response Team (CSIRT) at Incident@ihs.gov. If you have any questions about this article, please contact us at Cybersecurity@ihs.gov.