Adlumin

www.adlumin.com

5 SIGNS OF SOCIAL MEDIA VULNERABILITY

ADLUMIN, INC.

Let's start by accepting the inevitable: social media data breaches will happen, and your information may not be as private as you think. Cybercriminals are consistently looking for the weakest links, and social media has proven to be a significant vulnerability point for businesses and users. Social media usage is essential for businesses to keep up with brand promotion and build trust with their customers, making it a perfect place to target. As many of us use social media to share where we last vacationed or give career updates, cybercriminals are taking note. So, what makes someone an easy target? And how do cybercriminals choose who will be next? Let's take a deeper dive into what could potentially make you an easy victim.

1

OVERSHARING

Social media is a double-edged sword because we often exchange personal information online without thinking about who will access the data. However, there is a thin line between sharing and oversharing. Oversharing relates to exposing too much personal information online, including your address, location, account information, etc. The dangerous part about social media is that once content is out there, you have little to no control over how it is received and used by others. If you tend to put your personal information on your social media accounts, it is time to rethink.

2

LARGE FOLLOWER COUNT

Having a following, small or large, is a significant part of the social media experience. However, having too large of a follower count makes you a target for cybercriminals for many reasons. First, when you have a large following, you are more susceptible to having bots/ fake accounts following you. Secondly, by attacking an account with a large following, hackers will enter your account to access your followers. Once they obtain that access, they will try to take over other accounts you follow; it is a domino effect.

3

OUTDATED PRIVACY SETTING

Each platform consistently updates its privacy settings, and it is essential to know how your information is being used. The settings you choose specify if you give consent for collecting, using, and disclosing your personal information. Being in control of those settings could mean not handing over your data in the first place. A significant way to attempt to contain your personal information is to take advantage of and use the privacy settings.

4

ENABLE LOCATION

To share or not to share? Some geolocation tags can list your exact address. This means that you can share your precise location with anyone who follows you or your business on any of your social media accounts. If you show where you are, you're announcing that you are not home. Some cybercriminals target people for their physical possessions and can use enabled location to their advantage. Protect yourself and take control of who has access to your location by exploring the privacy settings within each platform you use.

5

INTERACTIONS / THRID-PARTY APP INTEGRATIONS

Over the years, without even realizing it, you have probably given third-party apps permission to access your information on different social media platforms. Many risks come with these permissions, including data breaches, newly granted end-users, compliance violations, regulatory violations, and more. It is essential to have control over your data, and it is highly recommended to regularly monitor third-party apps you are allowing to integrate within your environment.

The good news is that social media will continue to evolve and hopefully update its security settings along the way. The bad news is that cybercriminals will also develop, making it harder for businesses and individuals to steer clear of social media vulnerability. What's important to remember is that we are responsible for creating a secure experience for ourselves and businesses when navigating social media and online interactions. Always prioritize security, always safeguard your privacy because you never know what the alternative to not doing so will be.