RAYMOND JAMES

Protect your privacy on social media: How much is too much?

Follow these tips for protecting your privacy on social media.

In 2020, there were 3.96 billion active users on social media and the number keeps growing. Whether it's to find a place to eat, stay in touch with friends or family, or connect with industry peers to gain knowledge for your career growth, social media has a platform for you and your interests. But are you being safe with divulging your personal information, also known as personally identifiable information (PII)?

DON'T REUSE PASSWORDS

According to a Balbix report, 99% of users reuse passwords across either work accounts, personal accounts, or work and personal accounts. Using the same username and password across multiple applications increases your risk of identity theft and account compromise. We recommend using a password manager to hold all of your passwords. There are plenty of products available and some of them are even free. Be sure to read the product description to determine if it's the right fit for you.

WHEN SETTING UP YOUR ACCOUNT, ONLY SHARE REQUIRED INFORMATION

When you set up a social media account, you may be asked to provide your email address, date of birth, mailing address, place of employment and other personal details. Do you trust the platform with this information? Does it have a cybersecurity team to monitor and protect your PII from theft 24/7? Do they sell user information to third parties? The key is to only give out information that you feel comfortable with, and only provide the required information needed to sign up, even if a company asks for more.

LESS IS MORE WITH PROFILE PERSONALISATION

After you create your account, you may want to personalise your profile with pictures and biographical details like your location, birthday, workplace and position, and marital status. The more information you disclose about yourself, the more potential harm can be done by an attacker/ hacker. Passwords can be cracked just by looking at the information in someone's profile. For example, users may use a pet's name with their date of birth as a password, which is information that may have been shared in a post or profile.

UNDERSTAND WHO CAN SEE YOUR PROFILE AND POSTS

Who are you letting into your circle of friends, followers or connections? In multiple data breaches, hackers used fake social media accounts to befriend someone at the target company or send phishing links to gain insider information. If your profile is private and you receive a request from someone you do not know, validate that the person sending the request is actually who they say they are. You can always ask if they can set up a quick call to do an introduction or do a quick internet search of their name to see what pops up.

Once you hit the "post" button, your content is out there for anyone to see. If you post that you're going out of town or "check in" to restaurants or event venues, you only want those you trust to receive this information. Many burglaries can be traced back to homeowners sharing news about a holiday online.

If you can follow our tips above, you are on the right path to protecting your personal information and staying safe while surfing the web and using social media.