Five Best Practices to Follow on Social Media

By Wombat Security Technologies

There are many great things about social media, but there are also valid — and sometimes serious — security issues associated with these applications. **The following best practices can help you use social media safely:**

1. Understand – and frequently review – privacy settings

Social media is about making connections and facilitating the flow of information. As such, many applications default to lower privacy settings, making your profile and posts easy to find and engage with.

Make sure you understand how each application's settings can impact your privacy and adjust them accordingly. Privacy settings work differently on different platforms, and they can change frequently. Plus, features like "check-ins" and location tracking can reveal your schedule and habits. Do your due diligence up front and regularly circle back to ensure you're comfortable with how your data is being shared.

2. Assume everything you post is public and permanent

Seems contradictory to the first point, doesn't it? And, in a way, it is — but such is the double-edged sword of social sharing. Privacy settings can only protect you to a point.

Snapchat is a great example. Though the app now offers more options for its users, it's most recognized for messages known as "Snaps," which until recently would automatically disappear within 1 to 10 seconds of viewing.

The idea of "disappearing" messages is rather misleading, however, because recipients always have the option to take a screen shot of a Snap while viewing it. As such, any Snap could live for eternity and be shared with anyone. The same can be said of any post on any social sharing platform — regardless of privacy settings and regardless of whether the post was deleted. Screen captures and copy/paste functions can give posts a life beyond the limits you think you've set. So think very carefully about what you post online, no matter where you share it.

3. Be cautious of what you click

Malicious links and ads are everywhere online, and they frequently find homes on social media. From promises of free gift cards, to links to "pre-release" songs and movies, to teasers about the latest celebrity gossip, seemingly innocent links can get you into hot water. And that's before you take into account the potential pitfalls of shortened URLs, which reduce length (to help with character count restrictions) but eliminate visibility into where links actually lead.

Bottom line: Think before you click. Be as cautious on social media as you would with emails. If it seems odd, outlandish, or too good to be true, don't engage.

4. Watch out for imposters

Social engineers flock to social media in hopes of making inroads with unsuspecting users. Common techniques include the following:

- Creating fake profiles and connecting with users
- Building fake business accounts, pages, or sites, often taking advantage of known brand names to lure people in
- Hacking into existing accounts to gain access to friend lists and account information

Be mindful of these types of tricks and traps and steer clear of suspected imposters.

5. Choose connections carefully

Many privacy settings focus on protecting your data from the prying eyes of people, companies, and apps outside your accepted circle of connections, which means that all bets are off with regard to privacy protections inside that circle.

You should be selective about who you connect with on social media — after all, you don't want to end up giving an imposter access to your private life. One of the safest rules of thumb is to never connect with anyone you haven't met personally. Granted, you may regard this as impractical. Either way, carefully consider who you decide to share your life with via social media.

These best practices can help improve your social media savvy. However, if you are worried you have fallen for a scam or exposed confidential information, change your password(s) immediately and access the application's help pages and support forums as soon as possible. This can help minimize damage.

wombat®
security technologies
Change Behavior. Reduce Risk.