From the desk of
Carlos Kizzee
Vice President of Stakeholder Engagement

New Year, New Privacy Settings

While January 28, 2022 marks the 15th annual Data Privacy Day, each of us faces privacy concerns on a daily basis. If our private information becomes public, it can affect our credit ratings, employment options, and even our safety.

In this month's cybersecurity tips newsletter, we'll focus on steps you can take to maintain privacy on social media. If you're one of the lucky few who can live your life unplugged from Facebook, TikTok, and the like, you're in the clear. If you find yourself among the majority of us who either want or need to engage with others via social media, then here are some tips and tricks to stay safe and secure.

1 Protect Your Accounts

Social media accounts are under constant attack by cybercriminals. Your account can give a scammer a good way to infect your friends with messages that come from a trusted source (i.e., you). There are three simple steps you can take that will thwart most attacks:

- **Use long, unique passphrases:** Criminals get your account details from breaches and malware. If you use the same one everywhere, cybercriminals will have access to all of your accounts. Consider using a passphrase with multiple words, such as DenverIsBeautiful. It's easy to remember and tougher to crack.
- **Use Multi-factor Authentication (MFA):** MFA, sometimes called two-factor authentication (2FA) or advanced authentication, makes it almost impossible for someone else to log in to your account, even if they have your password. You trade the minor inconvenience of entering a one-time code for the huge benefit of keeping the baddies out of your stuff. Turn this on everywhere you can!
- **Update Everything:** Yes, everything. Keep your operating systems current on your computers, phones, apps, and internet-connected devices. Turn-on automatic updates and reboot when prompted. Networks are usually not compromised because of brand new, *0-day* vulnerabilities. Instead, they are breached because a patch was never installed for a bug that was fixed months (or years) prior.

2 Reduce Your Attack Surface

- Your attack surface is the sum of all the ways your information can be compromised. Every account with your personal data or app with a security flaw adds to it. You can reduce your potential vulnerability by deleting online accounts you no longer use and uninstalling apps you no longer need so they can't be used against you. With fewer things to manage and update, you can focus on protecting what is actually important.

3 Tweak Your Privacy Settings

- All major services offer privacy settings to limit what you share publicly. It may take a bit of exploration to find them, but you can use these tools to control your exposure. Pay special attention to location settings, permissions for facial recognition, who can tag you, and who can see your posts. Also, check the details you publish such as your hometown, birthday, family members, and where you work. Consider removing all of them.
- If it's allowed by the service you use, you can go a step further by not using real information, such as your full name or actual date of birth. Don't forget to check who can find you by your phone number and remember to also change your vanity name or username so it won't give you away.

4 Don’t Let Your Photos Betray You

- The photographs you upload to social media or share elsewhere online can expose your face, your address, the valuables you keep at home, the car you drive, and more. Keep this in mind before you post an image that might tell a stranger things you’d rather keep to yourself. Avoid sharing anything with your house number, license plate, or documents in view. For your kid’s safety, watch what they share online as well.
- Photos uploaded to major social media sites are scrubbed so that the metadata – hidden details that live within a picture or video file – are removed. Not all services protect you in the same way, and these metadata are always present when you email a file. Unless you disable the feature, your camera app is probably set to store your location which makes it easy for a criminal to see the exact latitude and longitude where a photo or movie was taken.

5 Would You Like to Know More?

These links will lead you to more resources to help protect your privacy:

- National Cybersecurity Alliance: Data Privacy Week
- FTC: Protecting Your Privacy Online
- CISA: Online Privacy Tips

Conclusion

- While it’s almost impossible to remain anonymous in 2022, there’s no reason to make it easier for criminals to take advantage of you. Information you share online, even if it’s restricted today, may go viral tomorrow. The best way to protect yourself is to avoid posting anything you wouldn’t want your grandmother to read in your local paper. You can’t regret a photo you never take.
- Once you upload a picture or write an angry tweet, you lose control of it, and anyone with a screenshot can continue to spread it long after you press the delete button. Search for yourself online every now and again to see what others will find when they look for you. Opt-out of any websites that share your personal details. Invest some time to ensure that a would-be attacker will be frustrated and move on to easier prey.
- Perfect privacy is impossible, but by being careful you can stack the odds in your favor. Stay safe, take care, and have a secure and Happy (Cyber) New Year!