November 2023

Monthly Security Tips Newsletter - Metropolitan Government of Nashville and Davidson County

Share with Care: Staying Safe on Social Media

No matter whether you're a pro influencer or a newbie with three followers, you need to think about cybersecurity and protecting your personal data while using social media. Nowadays, your Facebook, Twitter, Instagram, LinkedIn, TikTok and YouTube accounts are basically as critical as email, even if you don't post often. Here is how you can keep your account secure, enjoy your online social life, and ghost any scammer that slips into your DMs!

Prize your personal info

We want everyone out there to be snobby about sharing their personal data – there is nothing rude about it! Your data is worth billions to social media companies, but you can control what is collected. Your personal data is valuable, treat it like cash! Strike up a habit of paying attention to what data a social media platform is requesting (like your current location) and think about your answers.

Check your settings

Even if a social media app or website never asks you for data, you should assume it is still collecting it. Routinely (every month or so) check your privacy settings and ensure everything fits within your comfort level.

On mobile devices, social media apps might ask for you to give them access permissions at all times, but you don't have to agree. Here are some default settings you should usually turn off, unless you need it for the app to function and you trust the app:

- Camera – off
- Microphone – off
- Location – off
- Sync contacts – off

Enable MFA

Multi-factor authentication (MFA), sometimes called two-factor authentication or two-step verification, requires anyone logging into an account to prove their identity multiple ways. Typically, you will enter your username, password, and then prove your identity some other way, like with a fingerprint or by responding to a text message. Why go through all this trouble? Because MFA makes it extremely hard for hackers to access your online accounts, even if they know your password.

Passwords: Think long, strong, unique

Every one of your social media accounts should be protected by an awesome password created with these three guiding principles in mind:

1. Long: Every one of your passwords should be at least 12 characters long. Length is more important than complexity.

2. Unique: Each account needs to be protected with its own unique password. Never reuse passwords. This way, if one of your accounts is compromised, your other accounts remain secured.

3. Complex: Each unique password should be a combination of upper- and lower-case letters, numbers and special characters (like >,!?). Again, remember each password should be at least 12 characters long. Some websites and apps will even let you include spaces.

How do you keep track of all these unique passwords? Simple – use a password manager!

Share with care!

Be cautious about how much personal information you provide on social networking sites. The more information you post, the easier it may be for a hacker or someone else to use that information to steal your identity, access your data or commit other crimes such as stalking. Also, think about who can see your social media musings – most platforms allow you to limit who can see or engage with your posts if you don't know the whole world to know your business.

Posts are like ghosts

Even though many of us have been on social media for a decade or more at this point (maybe even most of your life!), it bears repeating that you should think about everything you post, message, or say online, because it can live forever. Posts are like ghosts; you don't want what you say to haunt you. This is true even for apps that automatically delete posts, like Snap. Someone who sees it can screenshot or screen-record what you post.

Be choosy about friends and followers

Remember that not everyone who requests to follow you has friendly intentions in mind. Depending on the information you have visible on your profile, someone who friends or follows you might know your contact info, general location, age, and other data. This is why you want to think twice before accepting a request or invitation to connect from just anyone. Many social media networks have tools that allow you to manage the info you share with friends in different groups. If you're trying to get your influencer hustle going, create an open profile or fan page that encourages broad participation but limits personal information. Use your personal profile to connect with your real friends – typically ones you know IRL.

Block the bullies!

While cyberbullying is often framed as an issue for children, anyone can be a victim. When it comes to the bullies of the 2020s, social media is now the unsupervised playground for us all. We recommend that you just block them – there's no need to give them more of your time and energy. Every platform has simple ways you can block and report users engaged in bullying behavior. There's no shame in having a strong blocking game!

Don't take the phishing bait!

Phishing is when cybercriminals use fake emails, social media posts, or DMs with the goal of luring you to click on a bad link or download a malicious file. If you click on a phishing link or file, you might hand over your data to hackers. A phishing scheme can also install malware onto your device. If you get suspicious, typo-ridden, or too good to be true messages from someone you don't know on social media, assume its phishing – delete it! You can usually report such messages to the social media platform, too. You might get a message or post from someone you know that seems like phishing ("when did Bill get into selling designer sunglasses?"). Assume it is phishing and delete. Use another method to contact the sender and let them know about the weird message.

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

STOP | THINK
CONNECT™

The information provided in the MS-ISAC Monthly Cybersecurity Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.