Social media plays a vital role in allowing people from all over the world to communicate almost instantly; however, it is critical to manage your digital footprint as well as the security and privacy settings on your accounts in order for your personal information to be accessible only to you. What you choose to share on social media is always your decision, but what others choose to do with your information may not always be in your control. Consider taking the following personal safety precautions with these social media safety tips.

Use Strong Passwords

Cyber-attacks are growing in complexity and frequency, which makes password choice more important than ever. A strong password is long, complex, and unique. The same password or versions of the same password should never be used across multiple accounts.

Here are some tips to increase your password security:

1. Include a combination of letters, special characters and numbers having a password length equal to a minimum of 16 characters – but not sequentially. For example, avoid 12345678.
2. Avoid any Personally Identifiable Information (PII) that can be found online, such as your birthday, school, family members or your dog's name!
3. If you use a dictionary word in your password, swap out some of the letters with numbers and symbols. For example, you can use 3 instead of E, or use zero instead of O.
4. Use a password generator to create and store strong, unique passwords in a secure vault. You'll only have to remember your one master password to access the others

Use Two-Factor Authentication (2FA)

If you require access to high-value or sensitive accounts and records such as company accounts or social media scheduling tools, you should add an extra layer of security to supplement usernames and passwords.

Time-based One-Time Password (TOTP) codes are a type of Two-Factor Authentication (2FA) that adds an important second layer of security to logins. To be authenticated, they require the user to enter a multi-digit verification code. The verification code is typically delivered via SMS text message or a third-party authenticator app such as Google Authenticator.

The two-factor authentication code ensures that the user is not impersonated.

Different Passwords for Social Media Accounts

Creating a different password for each of your online accounts may seem like a lot of work, but it's worth it to protect your data from cybercriminals. You can prevent compromised accounts by utilizing cybersecurity tools like password managers and multi-factor authentication.

There is more sensitive information than you might imagine stored in your social media accounts. For instance, shopping ads are constantly populating on our social media feeds. Only buy from reputable companies since when a purchase has been made through social media, your credit card information, email address and more sensitive data is saved within your social media account for future purchases. Because of this, if cybercriminals gain access to your social account, they'll also be able to get your credit card and other sensitive information.

Be Selective with Friend Requests

If you don't know the person, decline their invitation. It could be a fake account attempting to obtain personal information about you from browsing your profile. Keep it strictly to known family, friends and colleagues!

Don't Publish Personal Information

Don't provide any critical personal information, including your home address, credit card number or phone number. The more posts you make, the easier it is for cybercriminals to steal your identity.

Don't Share Travel Plans

It's common for people to post their next vacation on social media. After all, is it really a vacation if you don't document it on Instagram? However, doing so can put you at risk for a cyber-attack. You may be wondering how that's even

possible. Well, many cyber threats stem from social engineering attacks. Social engineering uses manipulation to trick you into giving away sensitive information. Cybercriminals use the information you provide on social media to plan their next attack. When you post about future travel plans, you give the cybercriminal ammunition to be their next victim. Some attacks go beyond the internet and could target your home since the attacker is aware that you will be gone for a period of time. To avoid being a victim of a social engineering attack, don't share your geolocation when traveling and always share the least information possible as you don't know who could be watching your activity through social media.

Use the Strongest Privacy Settings

Review the privacy settings carefully since some apps allow you to enable certain settings such as:

- Keep your profile private.
- Hide your friends.
- Hide your posts from the public.
- Disable search ability in Google and other search engines.

Some tools help control the amount of personal information you put online; others allow you to wipe the details of sites you have visited, or searches you have made, from your computer or device. For example, look for options that enable you to set your history to delete on a regular basis. Coordinate your settings so that they hold true across all of your devices.

Report, Block and Filter Content

Know how to report, block, and filter content. Read RAINN's tips on how to filter which users or content you see, report harmful comments or content, and block those who are attempting to use technology to hurt others.

Personalize Your Privacy Settings

Adjust your privacy settings on the site to your comfort level, and select options that limit who can view your information. Think about non-traditional social media as well, such as your public transactions on Venmo or music activity on Spotify. These site-specific security pages can help you get started.

- Twitter
- Instagram
- Facebook
- Pinterest
- Snapchat
- Tumblr
- LinkedIn
- Spotify
- Venmo

Pause Before You Post

Before you post, ask yourself if you are comfortable sharing this information with everyone who might see it. Content that contains personal information or your whereabouts could pose a safety risk. Even content that is deleted can sometimes be accessed by the website or through screenshots of the original post and could be used maliciously.

Turn Off Geolocation

Many social media sites or apps will request to access your location, but in most cases this isn't necessary. You can still get the most out of your social media experience without sharing where you are while you're there. If sharing where you are is important to you, consider waiting to tag the location until you leave. In addition to this, some sites may automatically make geotagged information public. When you "check in" on Facebook, update your Instagram story, or add a geotag to a Snapchat, these sites may share your exact location with people you may or may not trust with it. Take a look at the privacy settings on the sites listed above, or others you use regularly, to see what your location settings are and consider updating them.

Use A Private Internet Connection

Avoid public Wi-Fi connections, like those offered at coffee shops or airports, when using a website that asks for a password. Limit your social media usage to personal or private Wi-Fi networks, while using cellular data on your phone, or under the protection of a Virtual Private Network (VPN).

Talk to Your Friends About Public Posts

Let your friends know where you stand on sharing content that may include personally identifying information, like your location, school, job, or a photo of you or your home. Respect each other's wishes about deleting posts that may be embarrassing or uncomfortable. Always ask permission before you post something about another person, whether it mentions them indirectly, by name, or in a picture. To help keep track of your online presence, you can change your settings so that tagged photos of you will only appear on your profile—but won't be shared publicly on your timeline—if you have approved the post on Facebook or other social media accounts.

Report Harassment or Inappropriate Content

If someone is making you feel uncomfortable online, you can report the interaction to the host site, often anonymously. You can use the "report" button near the chat window, flag a post as inappropriate, or submit a screenshot of the interaction directly to the host site. If you do experience harassment or abuse through social media, consider taking screenshots immediately and saving them in case the content is deleted or removed from your view. To collect evidence of harassment on Facebook, you can download your full Facebook history through the Download Your Information (DYI) feature.

Look Before You Click

If you get a suspicious sounding message or link from a friend through social media, it's best not to automatically click it. Your friend's account may have been hacked, which could cause everyone in their contacts list to receive spam. If you're not sure it's spam, try contacting that person another way to ask if they meant to send you a link recently.

Make Privacy a Habit

Once you've gone through the privacy settings in your social media accounts, set a reminder on your calendar to revisit them in three or six months. Companies may change policies or update their platforms which could affect how you would like to share your information online.