Social Media Safety Tips

Social media platforms have become an integral part of our online lives. They are great for staying in touch with family and friends, but you should be wary about how much personal information you post. Cyber scammers and identity thieves are on those platforms as well. Here are some tips to help stay away from them.

1. **Lock Down Privacy Settings**

Privacy Settings are there to help you control who see what you post and manage your online experience in a positive way. Check your settings to make things such as your phone number and email addresses are hidden from public view. Here are a few platform-specific recommendations:

- Consider adjusting Facebook privacy settings to make your posts visible only to friends or friends of friends, rather than making them public.

- Uncheck the "Discoverability" boxes in Twitter's safety and security controls to prevent searches using your email address and phone number. If you're only using Twitter for private communications (as opposed to business networking), consider checking the "Protect your tweets" box, which limits your posts' visibility to your followers.

- On Instagram, if you plan to share personal images (and aren't promoting a business) consider setting your account to private.

2. **Use Two Factor Authentication** to Prevent Unauthorized Logins. This process can keep your accounts secure even if your username and password are stolen.

- Set up two-factor authentication on Facebook. Facebook also allows you to adjust various security settings, such as getting alerts for unrecognized logins (when someone logs in from a new device or web browser for the first time).

- Enable login verification on Twitter.

- Activate two factor authentication on Instagram

3. **Keep Your Personal Information Personal.** 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.

4. **Be Discreet About Your Whereabouts**

Take care to avoid sharing your street address, which can help thieves target your home. Also, be careful about broadcasting when you're traveling for extended periods when your vacant home could become a target.

Bear in mind that you can disclose this information inadvertently, without typing a thing, if you allow your posts or images to be tagged with your location. To prevent that, you can disable location tagging:

In Twitter, uncheck the "Tweet with location" box on the "Privacy and safety" settings page.

For the Facebook and Instagram mobile apps, you must go to your phone's settings, find location services, and disable them for the Facebook and Instagram apps.

(The process may differ somewhat from one manufacturer's phone to the next; if you have trouble finding the settings for your phone, consult your phone's user guide or online help pages.)

5. **Your Online Reputation can be a Good Thing**: Recent research also found that recruiters respond to a strong, positive personal brand online. So show your smarts, thoughtfulness and mastery of the environment.

- Once posted, always posted: What you post online stays online. Think twice before posting pictures or comments you wouldn’t want your parents or future employers to see.
- Recent research found that 70 percent of job recruiters rejected candidates based on information they found online.

6. Know and Manage Your Friends. Social networks can be used for a variety of purposes. Some of the fun is creating a large pool of friends from many aspects of your life. That doesn't mean all friends are created equal. Use tools to manage the information you share with friends in different groups or even have multiple online pages. If you're trying to create a public persona as a blogger or expert, create an open profile or a "fan" page that encourages broad participation and limits personal information. Use your personal profile to keep your real friends (the ones you know and trust) up to date with your daily life

- Be honest if you feel uncomfortable: If a friend posts something about you that makes you uncomfortable or seems inappropriate, let them know. Likewise, stay open minded if a friend approaches you because something you've posted makes him or her uncomfortable. People have different tolerances for how much the world knows about them respect those differences.
- Post only about others as you would have them post about you: The Golden Rule applies online as well.
- Know what action to take: If someone is harassing or threatening you, remove them from your friends list, block them and report them to the site administrator.

7. Avoid (and Report) Duplicate (Fraudulent) Friend Requests

If you receive a request to connect with someone you know, but who you thought was already a friend or follower, double-check your friends-list before accepting the invitation. If the sender is already on your list, chances are good their account has been hacked.

Scammers use bogus accounts cloned from real users to collect "friends," and rely on these "mutual friends" to extend their fake networks. The fake account may use photos from your friend's real account to trick you as well.

- Facebook has a provision for reporting these impostors that automatically notifies the friend who's being impersonated as part of the process.

- On Twitter and Instagram, impersonated persons have to report phony accounts themselves, so message your followers to let them know they're being misrepresented.

8. **Don't Use Social Credentials to Sign Into Third-Party Sites**

Many third-party websites give you the option of registering using Facebook, Google or Twitter credentials instead of setting up new usernames and passwords.

These shortcuts are tempting, especially when you're eager to place an order or join a discussion, but think twice. By using this option, you may be giving the new site more information than you need to.

Worse, if someone hijacks your social login information, they can gain access to these third-party accounts as well.

- If you've enabled access to third party sites in Facebook, you can review the sites that are logged in automatically by clicking "Apps" on the left side of the Settings page.

- You can shut off integration apps individually, or you can disable all integration with third-party sites and applications by changing a single setting.

9. **Avoid Quizzes and Games That Require Access to Profile Information**

"Fun" quizzes that promise to spot your perfect mate, assemble a bank-heist team, or test your hometown loyalty are often just information-siphoning schemes.

While assuring you they won't post to your feed without permission, they woo you into surrendering your profile info and friends. They can use this info to build lists for spammers.

10. **Handle Passwords With Care**

Don't store passwords in your web browser because if your phone or laptop is stolen, saved passwords can provide access to social accounts, shopping sites, and your email—all of which likely contain loads of information an identity thief could use. Another alternative is to password protect your computer.

- Switch up your social media passwords immediately if there's a chance you're the victim of a data breach or if you determine your personal

information is on the dark web. Use different passwords for each account site, and make sure they're strong.

- Ditch the sticky notes and index cards and upgrade to a better password management system. The helpful (and free) password manager, Dashlane works on Windows, Mac OS, iOS and Android. It encrypts and stores all your passwords (except its own), and lets you enter and submit them with a click.
- Make your passphrase a sentence: A strong passphrase is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember (for example, “I love country music.”). On many sites, you can even use spaces.
- Unique account, unique passphrase: Having separate passphrases for every account helps to thwart cybercriminals. At a minimum, separate your work and personal accounts and make sure that your critical accounts have the strongest passphrases.

11. Keep Security Software Current: Having the latest security software, web browser and operating system is the best defense against viruses, malware and other online threats.