FEBRUARY 2021 CCDC SAFETY MESSAGE

SOCIAL MEDIA SAFETY TIPS

Many of us use our social media platforms for a wide variety of communication. We set the programs up and then just automatically use them without revisiting our privacy and safety settings. Make privacy a habit by doing a regular social media privacy check-up. Once you have gone through the privacy settings in your social media accounts, set a reminder on your calendar to revisit them in three or six months. **Here are some updated tips to make your usage more secure.**

1. Lock Down Privacy Settings - Check the settings in your social accounts to make sure your phone number and email addresses are hidden from public view. Adjust your privacy settings on the site to your comfort level and select options that limit who can view your information.

2. Use Text Messaging to Prevent Unauthorized Logins - Consider supplying your smartphone number to each platform, and requiring it to use text messaging to confirm your identity when you log in on a new device **(two factor authentication**).

3. 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.

4. 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).

5. 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. By using this option, you may be giving the new site more information than you need to.

6. Be Discreet About Your Whereabouts - Take care to avoid sharing your street address or broadcasting your travel both of which can help thieves target your home. Also, disable location tagging.

7. Avoid (and Report) Duplicate 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.

8. Pause before you post - Before you post, ask yourself if you are comfortable sharing this information with everyone who might see it.

9. 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.

10. Look before you click - If you get a suspicious sounding message or link from a friend through social media, it is 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 are not sure it is spam, try contacting that person another way to ask if they meant to send you a link recently.

11. 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.

THINK SMART, BE AWARE, BE FLEXIBLE, BE EDUCATED (SAFE)