How-To-Document Resource:

How to stay safe on social media

Stay Safe on Social Media

Below are ten tips to increase your cybersecurity posture while using social media apps/sites

- **Pause before posting** - Only post information, such as photos, profile info, comments in blogs and forums, etc., you are comfortable with anyone seeing. Also, once you post information online, you may be unable to remove it altogether if necessary. Even if you remove the information from a site, saved or cached versions may still exist on other people's devices.
- **Be cautious of strangers** - The internet makes it easy for people to misrepresent their identities and motives. Consider limiting the people who are allowed to contact you on these sites. If you interact with people you do not know, be cautious about the amount of information you reveal.
- **Limit the personal information you post** - Do not post information that would make you vulnerable to a malicious actor, such as your address, birth date, schedule, or routine.
- **Talk with family and friends about public posts** - Let your family and 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.
- **Be Careful of Over - Friending and who you Friend** - As a member of a social networking group, it can be exciting to gain new "friends" or followers. Some "friends" can be problematic by introducing spam-posts and inappropriate posts. When accepting friends, choose people who are actual friends. Be careful of impersonators and unknown users attempting to gain personal information for malicious intent.
- **Report harassment and cyberbullying** - Many social media sites have a process to protect users from the intent of bullying or harassing of another person. If a photo or comment is intended to bully or harass someone, check the company's procedures to report abuse.
- **Turn off geolocation** – While many social media sites or apps will request to access your location, you can still receive the most out of your social media experience without sharing your location. 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.
- **Be wary of public Wi-Fi connections** - Avoid public Wi-Fi connections, like those offered at coffee shops or airports, when providing a password to a website such as your bank or credit card. 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).
- **Evaluate your settings** - Take advantage of a site's privacy settings. The default settings for some sites may allow anyone to see your profile, but you can customize your settings to restrict access to only certain people. Sites may change their options periodically, so review your security and privacy settings regularly to make sure that your choices are still appropriate.
- **Check privacy policies** – Similar to privacy settings, check the privacy policies of the website or app. Some online services may share information such as email addresses or user preferences with other companies. This can lead to an increase in email spam and increase the attack surface for a malicious