STAYING SAFE ON SOCIAL MEDIA

Beware of Your Content and Connections

Social media has become part of the everyday life of many Maine residents. While social media can be a fun and effective way of sharing information, connecting with the world around us, or seeing engaging content — it can also be used to snoop on personal information used in cyber attacks. Here are a few helpful tips about staying safe while enjoying the benefits of social media!





Don't share sensitive information.

Social media posts often reveal sensitive information in photographs as well as in written copy or video. Remember to protect information that could be used in a crime such as:

- **Travel plans and itineraries**
- **Home or business address**
- **License plate information**



Don't fill out social surveys.

Surveys and Quizzes are often used to gain access to your Password Reset or Banking Challenge Questions. Common surveys have titles like **"How well do you know me?"** These invite you to answer challenge questions such as **"What city was I born in?"** or **"What is my mother's maiden name?"** Unsuspecting people are often tricked into giving away personal data on friends and relatives.



Be skeptical of requests to connect.

It is common practice for cyber criminals and foreign government data collectors to connect with people based on where they work in an attempt to monitor them or request information. Don't accept requests to connect from people you don't know. Be suspicious of any request to share any information about your home or workplace.



Know where your data is stored.

TikTok is banned on Maine State Networks. When using social networks it is important to remember that not all data is stored in countries that respect your privacy. If you don't make an informed decision, your privacy and the privacy of the information entrusted to you could be compromised.



Understand algorithmic bias.

Social media companies earn money for ad clicks and media views. To maximize revenues, what you see is based on your likes and behavior in an attempt to get you to interact more with content. It is important to know that this business model may create a bias in the news, stories, and material you see.

It's time for your yearly social media health check!

1



Set privacy settings to most secure and most private.

- Use two-factor authentication and unique passwords for your social accounts that you don't use anywhere else.
- Restrict posts containing any personal information to be seen only by a limited audience that you've approved

2



Review your social media accounts from a public view.

- To see what is publicly available on your social accounts, view your social account from a browser that is not logged into any account. This simulates what any person could see, whether they are "friends" with you or not!

3



Review past posts for sensitive information.

- If you've had your social media account for more than a year it is important to go back and review your old posts for sensitive information and remove them. Did you post a license plate?

4



Close old or unused social media accounts.

- Social media applications come and go, but the information you leave on them stays. Remember to delete the accounts you no longer use.
- Limiting your digital footprint on the internet is a good idea, especially if those posts, images, and videos are on a platform you no longer use or monitor.

Pro tip: **Many identity theft protection companies will monitor your social media accounts as part of your paid service! This is an excellent way of protecting your social accounts.**

CYBER DEFENSE SERVICES A+OM

MUNICIPAL CYBER DEFENSE PROGRAM POWERED BY ATOM

Brought to you by the **State of Maine**