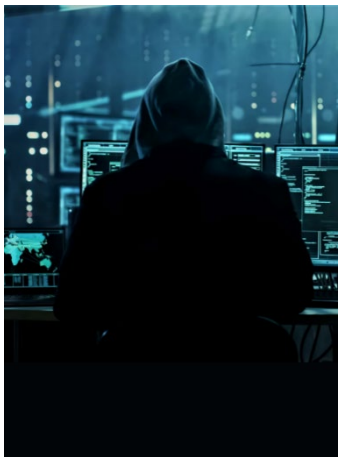
# CYBER SECURITY KEYPOINTS September

***From the County Network Security Cooperative***


## 6 Tips and Best Practices

1. POSTING PERSONAL INFORMATION
   - When posting personal information about yourself, keep the highest privacy settings and consider what you are posting.
2. REVIEW WHAT OTHERS POST ABOUT YOU
   - Review, if possible, what others publish about you on their own sites and social media. Contact the website's abuse center if necessary. Be aware that photos, videos and private chat sessions can easily be shared.




3. MANAGE PRIVACY SETTINGS
   Most social networking sites offer privacy controls. Make use of them and review them often as they can change and are often complex.
4. BE WARY OF THIRD-PARTY APPS AND GAMES
   Be careful of third-party programs and apps as they can be used to infect or access your computer.
5. KNOW WHO TO TRUST
   Only accept friends or contacts you know and review their account to ensure they haven't been hacked.
6. USE MULTI-FACTOR AUTHENTICATION (MFA)
   Most social media sites offer multi-factor authentication (MFA). Always turn MFA on in your settings to keep your account secure.

## Staying Safe on Social Media

Social media has become a haven for hackers because they encourage you to share your personal information. These sites are designed to allow you to interact and share as easily as possible. Still, if you're not careful, their use can leave you vulnerable to identity theft, viruses, malware, privacy violations and more.

## Did you know?

**In 2023, 25% of Facebook accounts were hijacked, while the hacking percentage of Instagram accounts reached 85%. Facebook accounts are the most compromised account types in the United States, reaching around 67,941 every month.**

The County Network Security Cooperative is a collaboration of partners including:

- AND -

NIRMA Serving County Government

Disclaimer: This document reflects current guidance and is subject to change due to the evolving cyber security environment.