Cybercrime Prevention Flyer

CPF 00017-2021-CID361-9H 30 November 2021

Social Networking Safety Tips

Social networking is an integral part of daily life for many people. As a result, people really do not think much about how their social media accounts are set up or what they share. Unfortunately, this familiarity reduces a person's inhibitions and people become lax in their social networking vigilance.

Cybercriminals, on the other hand, are always on the lookout for, and ready to exploit, gaps in a social media user's attentiveness to secure their social media accounts or what the user posts. With some simple information, cybercriminals can create profiles, compromise accounts, and commit fraud, netting thousands of dollars or more and making life difficult for the victim.

Taking some simple steps, social media users can better protect themselves from becoming the next cybercrime victim.

- **Keep antivirus software up to date.** Social media companies protect their websites from malicious content, but they do not scan the websites of links posted by their users.
- **Be wary of clicking a link in a post.** The link, which can be made to look legitimate, could lead to malicious content. To provide a sense of security and verify possible link safety, copy and paste the link into a free online virus scanner.
- **Enable two-factor authentication.** Two-factor authentication makes it harder for cybercriminals to gain access to online accounts. Even if a password is compromised, the password alone will not be enough to pass the authentication check.
- **Do not use the same password for all accounts.** A single leak of that password could put all accounts at risk. Use long, strong, and unique passwords; passphrases are even better than passwords for additional security.
- **Not everyone is who they say they are on social media.** Criminals create fake profiles in order to collect information and scam people. So, be selective and verify identities when deciding to associate with someone via social media and do not accept friend requests from strangers.
- **Do not share too much information.** Sharing too much—a birthplace and date, home address, phone number, a maiden name, work information, etc.—on a profile or in a post makes it easier for a criminal to use that information to create a fake profile, answer security questions, or commit fraud.
- **Be careful when posting images.** Posting images to social media might reveal more personal details about yourself than you think or want to. An image of a birthday celebration could identify a date of birth. Images of a new home could give cybercriminals

Report a crime to U.S. Army Criminal Investigation Division

Major Cybercrime Unit

27130 Telegraph Road
Quantico, Virginia 22134

Email

MCU Web Page

CID LOOKOUT
ON POINT FOR THE ARMY

"DO WHAT HAS TO BE DONE"

location information or home details. Selfies or family images provides family details and the images can be used to create fraudulent accounts.

- **Do not use the default social media privacy settings.** Customizing the privacy settings gives the social media user more access control to their information.
- **Use a virtual private network (VPN).** A VPN provides a protected, encrypted, network connection.
- **Conduct name, profile, and username searches.** Doing this identifies what cybercriminals will see if they conduct a similar search.
- **Remember, what is posted on the internet is permanent.**

Social networking will continue to have a significant place in daily life, similar to cell phones, which people are reluctant to hand over, even to family members and friends. So, do not hand over your social media profiles or content to the general public or to criminals.

For additional information, we encourage our readers to visit the websites listed below. If you believe your social media account has been compromised or you are aware of a fraudulent account, report it to the social media provider.

Facebook Help Center: Staying Safe

Twitter Help Center: Safety and Security

Instagram: Privacy, Safety and Security

Snapchat Support: Staying Safe on Snapchat

LinkedIn: Safety Center

Department of Homeland Security: Using Social Media Safely

Cybersecurity and Infrastructure Security Agency: Staying Safe on Social Networking Sites

Cybersecurity and Infrastructure Security Agency: Social Media Guide

Virginia National Guard: Online Safety and Security Tips and Resources

Twitter Safety Tips

LinkedIn Safety Tips

Facebook Safety Tips

To receive future MCU Cybercrime Prevention Flyers, send an email to: Subscribe CPF