Personal Safety & Security

Social Media

Personal Safety & Security
YOUR SAFETY OUR PRIORITY

The safety and security of Federal employees and those who visit Federal facilities is the Federal Protective Service's mission and top priority. As co-chair of the Government Services and Facilities Sector, FPS promotes security and resilience by sharing information and resources sharing with state, local, tribal, and territorial government personnel.

SOCIAL MEDIA SAFETY

While social media platforms are excellent tools for connecting and sharing information, features like user profiles, timelines, status updates, friend lists, and messaging services can allow dangerous actors to gain insights into your daily activities. This information may be used to disrupt your life or target you, your colleagues, or your family. The following guidance can help you take a proactive approach to protecting against online threats.

HOW TO PROTECT YOURSELF ON SOCIAL MEDIA

1. **Be cautious.** Limit the amount and type of information you provide to companies and online services. Consider if the information requested is necessary for the service and only provide the minimum. Scrutinize unknown connections, followers, and contacts. Cyber criminals can use fake profiles and websites to elicit information.
2. **Protect your passwords.** Protect your accounts by using strong, regularly updated and unique passwords. Consider using a password manager to help store them securely, and enable multi-factor authentication whenever possible, which adds an extra layer of security by requiring a secondary form of verification.
3. **Think like the adversary.** Put yourself in the bad actor's shoes by running searches of your own name through commercial search engines. Use different combinations of your name and other information, such as your address, screen/profile names. Leverage private browsing modes to see what the public—and a potential exploitative criminal—can see.
4. **Opt out.** Once you review the results of your self-searches, consider taking action to opt out or request removal of your. Log into your social media accounts/profiles and adjust the settings of who can view your profile, posts, and other information. Be sure to review your profile settings on your mobile devices, too. This will help you determine the level of sharing you have opted into.
5. **Stay private.** Review privacy policies and limit use of third-party applications on social media to log into other accounts. These third-party applications receive personal identity information from your profile when you use them. Depending on the platform's terms of service, you can opt out or decline to have this information shared. Some social media sites send your email address or other preferences to companies for marketing purposes.

For additional information and helpful tips, tools, and other help to protect you, your family, and your business from online threats, check out the Cybersecurity and Infrastructure Security Agency's (CISA) Secure Our World program. From updating software to recognizing the latest phishing scams, this national public awareness campaign from CISA provides invaluable resources to help you take control of your online safety through simple steps.

Be sure to visit Secure Our World at CISA.gov/Secure-Our-World.

CONTACT THE FPS MEGACENTER TO REPORT ANY SUSPICIOUS ACTIVITY:

1-877-4FPS-411 (1-877-437-7411)
OR CONTACT YOUR LOCAL AUTHORITIES
****DIAL 911 FOR EMERGENCIES*

Resources for victims of crime: dhs.gov/victims-crime

FEDERAL PROTECTIVE SERVICE
FPS

Connect on social media @FPSDHS
Learn more at DHS.gov/FPS
Scan QR code to visit DHS.gov/Publication/YourSafetyOurPriority