Social Media Dos and Don'ts

Security Dos and Don’ts on Social Media

Employees are reminded to use caution when using social networking sites, such as Facebook or Twitter. Please keep the following in mind:

Do:

- Be aware that if your **personal** social networking profile is not set to “private”, anyone will be able to see your profile and everything that you post. For more information about social networking privacy settings, contact the Department’s Bureau of International Information Programs, Office of Innovative Engagement (IIP/OIE) at OIESupport@state.gov.
- Be very careful about posting photos that may contain sensitive information such as clues to locations or personal information in the background.
- Beware of malicious code from third-party applications.

Don’t:

- Don’t post Department PII, SBU, or classified information on personal social networking sites.
- Don’t post or Tweet photos that could compromise physical or operational security (e.g., photos of Department facilities, buildings, grounds, gates, or badges).
- Don’t expect that your information will be private on any social networking sites; hackers and other bad actors may still be able to access this information.

For additional resources please e-mail AFSA@state.gov.

Contact awareness@state.gov if you have any questions.