

West Virginia Executive Branch Privacy Tip of the Week

Periodically, the Privacy Office may issue tips for the purpose of assisting you in making informed decisions in your “away from work” life. The following tip is for that purpose (most of us know that we cannot visit social networking sites for personal use while on the job and with State equipment!)

Consider the Risks of Using Social Networking Sites

Social networking websites like Facebook and MySpace make it easy to share information and photos with business associates, family, friends, and old classmates. Unfortunately, YOUR personal information on social networks is also attracting people with ulterior motives. The appropriate balance must be found between exposing your personal information and the benefits gained from using these services.

Here are some points to keep in mind as you consider using various social networking sites:

- Do not rely on default settings, as these often permit strangers to view details that you would typically not share with someone unknown to you. Always exercise discretion. The best way to protect your personal privacy is to use common sense, caution, and skepticism.
- Understand the security and privacy features available for the social networking sites you use and use appropriate restrictions. Available privacy settings change periodically so be sure to stay up to date and change your settings appropriately.
- Do not grant access to your email account. Social networks often want users to provide logon credentials to their e-mail account (including password) so they can access the user’s e-mail address book in order to solicit your contacts to join. Once you provide those credentials, that network site has access to your e-mail account as well as all of your friends’ and colleagues’ email addresses.
- Your place and date of birth are useful data to identity thieves. While sites need to collect birth dates to ensure they are not soliciting minors, you should not permit sites to display your full date of birth.
- Beware of posting your location using location-aware, GPS enabled applications. Consider the security risks of telling the world where you are. If the value of the service does not outweigh the risks, do not use these features. Remember, no matter how carefully you construct your privacy settings, there’s no guarantee that what you post won’t become known to unauthorized viewers.

- Do not post compromising information or pictures. Remember that whatever goes on a network might eventually be seen by people who were not in the intended audience. Think about whether you would want a stranger, an insurance agent, the government, your mother or a potential employer to see your posts or pictures. Employers have been known to rule out job candidates after researching them on social sites. If someone posts a picture of you, do not be afraid to ask to have content removed if you believe it does not reflect well on you.
- Never use the same password for multiple online accounts. A breach of one account could create vulnerability in other places you log on, such as banking, brokerage, credit card, or other financial sites.

For more information on social networking privacy see “Social Networking Privacy: How to be Safe, Secure and Social”: <http://www.privacyrights.org/social-networking-privacy>.