

SECURITY - Now ...more than ever!

Cyber Security - Disaster Recovery - Continuity of Government



DTI eSecurity News – Using Social Networking Sites Safely

Social Networking Sites Come With Risks



Nearly everyone is familiar with social networking sites like Facebook, Twitter, and Pinterest, which many of us use daily. They let us meet, interact, and share with people worldwide. However, all of this access comes with risks, not only for the user, but for family, friends, and even employers.

Produced in part from [SANS](#)

What Are The Privacy Concerns?

A common concern about social networking sites is protection of personal information. The best protection is limiting the information you post. The privacy of your information is only as secure as the people you share it with. Be aware of what information friends are posting about you and respectful of what you post about others. Potential privacy dangers include:

- **Future Impacts:** As part of background checks, organizations may search social networking sites. No matter how old they are, embarrassing or incriminating posts could prevent you from getting hired or promoted. Also, many universities conduct similar checks for new student applications.
- **Attacks Against You:** Cyber criminals can harvest your personal information and use it for attacks against you. They can use your information to reset your online passwords, create targeted email attacks (spear phishing), or apply for a credit card using your name.
- **Harming Your Employer:** Criminals or competitors can use sensitive information you may post about your organization against your employer. Your posts can potentially cause reputational harm for your organization. Check policies before posting anything about your employer.

What Security Protections Should You Use?

Social networking sites can be used by cyber criminals to attack you or your devices. Here are some steps to protect yourself:

- **Login:** Protect your social networking account with a strong password. Do not share this password with anyone or re-use this password for other sites.
- **Encryption:** Many social networking sites allow you to use encryption (HTTPS) to secure your connection to the site. Whenever possible, use HTTPS.
- **Email:** Be suspicious of emails that claim to come from a social networking site; they can easily be spoofed by cyber criminals. Do not reply to these emails; instead, login to your social networking site directly, and check messages or notifications from within the website.
- **Malicious Links/Scams:** Be cautious of suspicious links or potential scams posted on social networking sites. Cyber criminals can post malicious links which, if clicked on, can take you to websites that attempt to infect your device.
- **Apps:** Some social networking sites give you the ability to add or install 3rd-party applications, such as games. Keep in mind there is little or no quality control or review for these apps. Only install apps if you need them and if they are from well-known trusted sites. Remove them when you no longer need them.

Visit the [eSecurity Extranet](#) website for previous issues of

[eSecurity Newsletters](#)

Keep an eye out...

If you spot the DTI/Verizon/DART
Cyber Bus on the road...

Send us a picture on Twitter



[@DeldigiKNOW](#) to qualify for a monthly prize



Questions or comments?

E-mail us at eSecurity@state.de.us