



DTI eSecurity News – Staying Safe On Social Networking Sites



The popularity of social networking sites, such as Facebook, LinkedIn, Twitter, and others, has expanded in recent years. According to the [Pew Internet & American Life Project](#), 65% of Americans are using these sites on a regular basis. Unfortunately, the sites continue to serve as prime targets for spam distribution and phishing scams. In 2011, a [Barracuda Labs Survey](#) reported that over 91% of respondents received spam and over 54% were targets of phishing attacks on social networking sites. There is a greater need for remaining vigilant while on these sites.

Produced in part from [MS-ISAC](#)

What Are Security Concerns?

Social networking sites continue to grow in popularity for attacks because of the volume of users and the amount of personal information posted.



The very nature of the sites encourages posting of such information. The perceived anonymity and false sense of security of the Internet may cause users to post more information about

themselves and their life than they would provide to a stranger in person.

Information posted could be used by people with malicious intent to conduct social engineering scams and attempt to steal your identity. Individuals are tempted to click on a video they see on a friend's page, but these videos may lead to a malicious website which could infect your device.

Remember: If you wouldn't wear it, don't share it online.

What Can You Do To Be Safe?

- **Keep systems updated.** Ensure that any device you use to connect to a social networking site has proper security measures in place and that they are kept up-to-date. The default should be set to "auto update" so patches can be applied automatically without intervention.
- **Use strong passwords.** Protect your social networking account with a strong password. Do not share the password with anyone or use it for other sites. Some social networking sites support features for stronger authentication, such as using one-time passwords when logging in from public computers or using your phone as part of the login process.
- **Links.** Be cautious when clicking on links. If a link seems odd, suspicious, or too good to be true, do not click on it...even if the link is on a trusted friend's page.
- **Scams.** Criminals take advantage of the open nature of social networking sites to defraud individuals. Be cautious when contacted on a social networking site with a request for money or with an offer that's surprisingly good.
- **Privacy.** Do not assume privacy on social networking sites. Confidential information should not be shared. Review a site's privacy policy. If a site's privacy policy is vague or does not properly protect your information, do not use the site.
- **Personal Information.** Do not respond to an email requesting personal information or asking you to 'verify your information' or 'confirm your user ID & password'.
- **Be cautious about installing applications.** Only install applications that come from trusted, well-known sites. Installing some applications may modify your security and privacy settings. If you are no longer using the app, REMOVE it.

DID YOU KNOW? Newsletters

Public versions of the DTI eSecurity Newsletters are available on the [Delaware Cyber Security Internet web page](#).

Questions or comments?
E-mail us at eSecurity@state.de.us