



Action Item Checklist for Facebook Safety

- Know the four types of Facebook users – Friends, Outsiders, Businesses, and Enemies.
- When logging in to Facebook, be sure you are on the right website. If you are worried you are on a site impersonating Facebook, type www.facebook.com into your web browser to be sure.
- Use a case-sensitive complex password for your profile that includes numbers, letters, and symbols – e.g. \$uNf)0w3R.
- Before you share information online about yourself or your workplace, ask yourself this question: What would the consequences be if this information fell into the hands of my worst enemy, competitor or boss?
- Be conscious of all the information (phone number, address, Date of Birth, password reminders) on your Facebook Profile and the potential hazards it could cause you. Read 10 types of Information to Keep Private.
- Read the Facebook privacy policy and privacy help page.
- Secure, understand and customize your Privacy Settings. Double-check your settings each time Facebook makes and update to be sure you aren't sharing anything by default.
- Avoid taking Quizzes, adding unknown applications and joining unknown or unnecessary Groups.
- Post updates, photos, videos and identity as if your favorite grandparent, future boss and worst enemy were watching.
- If they aren't your friend, don't pretend. Don't accept friend requests unless you are absolutely sure you know who they are and that you would associate with them in person.
- Maintain a healthy skepticism of social networking. Verify, then trust.
- Understand Facebook Places and how to deactivate location sharing.
- Know the difference between Deleting and Deactivating your Facebook Account and how to do both.
- Stay Up-to-date on any changes to Facebook or other Social Networking sites so you are informed and protected.
- Share your knowledge and this information with your Facebook Friends. The more informed all users are – the safer the social networking community is!
- Be aware (and discrete) about the information you share about others. Next time it might be them sharing about you.