CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION
Internet Crime Complaint Center
Private Industry Notification

May 29, 2014

(U) Law enforcement has become aware that foreign cyber adversaries are utilizing popular social network sites to assess, target and successfully conduct computer network exploitation activities against:

- US federal, state and local government and private academic and industry networks
- Individual employees of US federal, state and local government and private academic and industries
- Family members and personal and/or professional associates of these employees and private citizens with high visibility

It is advised that industry use due diligence to inform and educate their associates on the vulnerabilities associated with the use of social networking sites.

(U) What are social network sites?

The US-Computer Emergency Readiness Team (US-CERT) defines Social networking sites, referred to as "friend-of-a-friend" sites, as “where you are connected to new people through people you already know. The purpose of some networking sites may be purely social, allowing users to establish friendships or romantic relationships, while others may focus on establishing business connections. Although the features of social networking sites differ, they all allow you to provide information about yourself and offer some type of communication mechanism (forums, chat rooms, email, and instant messenger) that enables you to connect with other users. On some sites, you can browse for people based on certain criteria, while other sites require that you be ‘introduced’ to new people through a connection you share. Many of the sites have communities or subgroups that may be based on a particular interest.” http://www.us-cert.gov/ncas/tips/ST06-003

The three most popular social network sites are Facebook, Twitter, and LinkedIn.

(U) The following are security tips on the use of social network sites from US-CERT:

How can you protect yourself?

- **Limit the amount of personal information you post** - Do not post information that would make you vulnerable, such as your address or information about your schedule or routine. If your connections post information about you, make sure the combined information is not more than you would be comfortable with strangers knowing. Also be considerate when posting information, including photos, about your connections.

- **Remember that the internet is a public resource** - Only post information you are comfortable with anyone seeing. This includes information and photos in your profile and in blogs and other forums. Also, once you post information online, you can't retract it. Even if you remove the information from a site, saved or cached versions may still exist on other people's machines (see Guidelines for Publishing Information Online or http://www.us-cert.gov/ncas/tips/st05-013 for more information).

CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION
Internet Crime Complaint Center
Private Industry Notification

- **Be wary of strangers** - The internet makes it easy for people to misrepresent their identities and motives (see Using Instant Messaging and Chat Rooms Safely or http://www.us-cert.gov/ncas/tips/st04-011 for more information). Consider limiting the people who are allowed to contact you on these sites. If you interact with people that you do not know, be cautious about the amount of information you reveal or agreeing to meet them in person.

- **Be skeptical** - Don't believe everything you read online. People may post false or misleading information about various topics, including their own identities. This is not necessarily done with malicious intent; it could be unintentional, an exaggeration, or a joke. Take appropriate precautions, though, and try to verify the authenticity of any information before taking any action.

- **Evaluate your settings** - Take advantage of a site's privacy settings. The default settings for some sites may allow anyone to see your profile, but you can customize your settings to restrict access to only certain people. There is still a risk that private information could be exposed despite these restrictions, so don't post anything that you wouldn't want the public to see. Sites may change their options periodically, so review your security and privacy settings regularly to make sure that your choices are still appropriate.

- **Be wary of third-party applications** - Third-party applications may provide entertainment or functionality, but use caution when deciding which applications to enable. Avoid applications that seem suspicious, and modify your settings to limit the amount of information the applications can access.

- **Use strong passwords** - Protect your account with passwords that cannot easily be guessed (see Choosing and Protecting Passwords or http://www.us-cert.gov/ncas/tips/st04-002 for more information). If your password is compromised, someone else may be able to access your account and pretend to be you.

- **Check privacy policies** - Some sites may share information such as email addresses or user preferences with other companies. This may lead to an increase in spam (see Reducing Spam or http://www.us-cert.gov/ncas/tips/st04-007 for more information). Also, try to locate the policy for handling referrals to make sure that you do not unintentionally sign your friends up for spam. Some sites will continue to send email messages to anyone you refer until they join.

- **Keep software, particularly your web browser, up to date** - Install software updates so that attackers cannot take advantage of known problems or vulnerabilities (see Understanding Patches or http://www.us-cert.gov/ncas/tips/st04-006 for more information). Many operating systems offer automatic updates. If this option is available, you should enable it.

- **Use and maintain anti-virus software** - Anti-virus software helps protect your computer against known viruses, so you may be able to detect and remove the virus before it can do any damage

CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION
Internet Crime Complaint Center
Private Industry Notification

(see Understanding Anti-Virus Software or http://www.us-cert.gov/ncas/tips/st04-005 for more information). Because attackers are continually writing new viruses, it is important to keep your anti-virus definitions up to date.

For more information on the use of social network sites, please visit US-CERT website www.us-cert.gov

(U) Additional US-CERT Resources:

- Staying Safe on Social Network Sites (http://www.us-cert.gov/cas/tips/ST06-003.html)
- Guidelines for Publishing Information Online (http://www.us-cert.gov/ncas/tips/st05-013)

(U) Other Resources

- Seven Deadly Sins of Social Network Security (http://www.csoonline.com/article/496314/seven-deadly-sins-of-social-networkingsecurity)
- Social Networking and Security Risks (http://www.gfi.com/whitepapers/Social_Networking_and_Security_Risks.pdf)
- Risks and Benefits of More Open Social Networking (http://www.epa.gov/oei/symposium/2010/gotta.pdf)

(U) Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI Cyber Task Force or Cyber Watch (CyWatch), by telephone at 855-292-3937 or by e-mail at cywatch@ic.fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

You can also report suspicious online activity to the FBI's Internet Crime Complaint Center at http://www.ic3.gov