THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Office of Research Security Newsletter

May 1, 2017

Welcome

Most computer infections come from websites. Just visiting a website can expose your computer to malware even if you do not download a file or program. Often legitimate sites may be unknowingly infected. Websites with information on popular celebrities or current sensational news items are frequently hijacked by criminals, or criminals may create such websites to lure victims to them.

Vulnerability of Social Networking Sites

Social networking sites are Internet-based services that allow people to communicate and share information with a group.

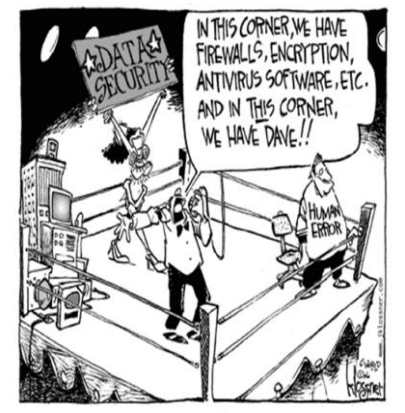
Risks:

Once information is posted to a social networking site, it is no longer private. The more information you post, the more vulnerable you may become. Even when using high security settings, friends or websites may inadvertently leak your information.

Personal information you share could be used to conduct attacks against you or your associates. The more information shared, the more likely someone could impersonate you and trick one of your friends into sharing personal information, downloading malware, or providing access to restricted sites.

Predators, hackers, business competitors, and foreign state actors prowl social networking sites looking for information or people to target for exploitation.

Information gleaned from social networking sites may be used to design a specific attack that does not come by way of the social networking site.



Social Networking Dos & DON'Ts

- Establish and maintain connections with people you know and trust; review your connections on a regular basis.
- Assume that ANYONE can see information you post about your activities, location, and personal and professional life.
- Make sure your family takes similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting or tagging images of you or your family that clearly show your face.
- Post pictures taken at a distance or angle that conceals your identity.
- Use secure browser settings when possible, and monitor your browsing history to ensure that you recognize all access points.

BE ALERT!

Assume anyone can see information you post about your activities, location, and personal and professional life, regardless of your privacy settings.

Insider Threat

The Insider Threat is current or former employees, contractors, or business partners, with authorized access to company information who misuse that information for their own benefit or that of a competitor or foreign nation.

Possible motivations can include greed or financial need, revenge, ideology, divided loyalties, ego, vulnerability to coercion, etc. Some behaviors which might indicate insider activity include:

- Seeking to expand access beyond job requirements
- Sudden reversal of financial situation
- Outward disgruntlement towards employer
- Paranoia that they are under investigation
- Working odd hours inconsistent with job assignment
- Unreported foreign contacts or foreign travel (when required)
- History of security infractions or indifference to policies

Employee Countermeasures

Employees are the first line of defense in safeguarding classified information. Some simple ways to lower your risk of recruitment and better fulfill your responsibilities as a cleared employee include:

- Maintain a responsible and professional social networking footprint.
- Refrain from identifying yourself as a cleared employee on social or professional networking sites.
- Always utilize encryption when sending sensitive email communications.
- Never release company information beyond what's publicly available.
- Adhere to all company and customer IT policies and procedures.
- Never discuss sensitive information in public places (i.e. restaurants, public transportation, trade shows, etc.).
- Don't respond to questionable electronic communications.
- Maintain a keen awareness of surroundings; notify security of any anomalies or concerns.