THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Office of Research Security Newsletter

February 1, 2018

SAVE THE DATE – April 4 Security Refresher Training
at the Chan Auditorium. It will count for BOTH their export & refresher security training. More details to come.

Your Social Media Habits Could Soon Affect Your Security Clearance

By Lindy Kyzer, Government Executive, May 27, 2016

Social media checks should not change the status quo for security-cleared professionals or applicants. It is still critical to follow safe social networking, to protect your private information and not post things you wouldn't want your boss or a recruiter to see. But, for applicants with borderline issues, social media checks may provide the tipping point that leads to a clearance denial. A single DUI alone would likely not flag your alcohol consumption as a potential security risk. But that, along with a variety of photos on social media sites that shows you inebriated or in compromising situations, may cause your clearance to be denied or revoked. (Excessive alcohol consumption is an adjudicative criterion currently considered by investigators.)

Read Full Story Here:
http://www.govexec.com/excellence/promising-practices/2016/05/your-social-media-habits-could-soon-affect-your-security-clearance/128647/#.WIaAU4m5OYA.email

Upcoming Trainings for 2018 Bob Jones Auditorium, Redstone Arsenal:

- **May 15, 2018** – 11:30 am to 1:00 pm, Threat Awareness CI
- **August 7, 2018** – 11:30 am to 1:00 pm, Threat Awareness CI
- **October 3, 2018** – 11:30 am to 1:00 pm, Threat Awareness CI

REMINDER – It is IMPORTANT to keep ORS updated with the correct contact information "email, phone, work location". This is critical in maintaining your Personnel Security Clearance (PCL) or NASA/MSFC Accesses

Tips on How to Protect Your Home Computer

- **Keep Your Firewall Turned On**
  A firewall helps protect your computer from hackers who might try to gain access to crash it, delete information, or even steal passwords or other sensitive information. Software firewalls are widely recommended for single computers. The software is prepackaged on some operating systems or can be purchased for individual computers. For multiple networked computers, hardware routers typically provide firewall protection.
- **Install or Update Your Antivirus Software**
  Antivirus software is designed to prevent malicious software programs from embedding on your computer. If it detects malicious code, like a virus or a worm, it works to disarm or remove it. Viruses can infect computers without users' knowledge. Most types of antivirus software can be set up to update automatically.
- **Install or Update Your Antispyware Technology**
  Spyware is just what it sounds like—software that is surreptitiously installed on your computer to let others peer into your activities on the computer. Some spyware collects information about you without your consent or produces unwanted pop-up ads on your web browser. Some operating systems offer free spyware protection, and inexpensive software is readily available for download on the Internet or at your local computer store. Be wary of ads on the Internet offering downloadable antispyware—in some cases these products may be fake and may actually contain spyware or other malicious code. It's like buying groceries—shop where you trust.
- **Keep Your Operating System Up to Date**
  Computer operating systems are periodically updated to stay in tune with technology requirements and to fix security holes. Be sure to install the updates to ensure your computer has the latest protection.
- **Be Careful What You Download**
  Carelessly downloading e-mail attachments can circumvent even the most vigilant anti-virus software. Never open an e-mail attachment from someone you don't know, and be wary of forwarded attachments from people you do know. They may have unwittingly advanced malicious code.
- **Turn Off Your Computer**
  With the growth of high-speed Internet connections, many opt to leave their computers on and ready for action. The downside is that being "always on" renders computers more susceptible. Beyond firewall protection, which is designed to fend off unwanted attacks, turning the computer off effectively severs an attacker's connection—be it spyware or a botnet that employs your computer's resources to reach out to other unwitting users.
- **Implement Strong Passwords on all Network Devices**
  In addition to a strong and complex password on the wireless access point, a strong password needs to be implemented on any network device that can be managed via a web interface. For instance, many network printers on the market today can be managed via a web interface to configure services, determine job status, and enable features such as email alerts and logging.