The Purple Dragon

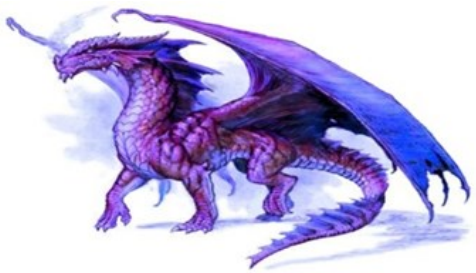
Joint Information Operations Warfare Center
Joint OPSEC Support Element (JOSE)
"A Chairman's Controlled Activity"

Volume 27 Fall 2015

Inside this issue:

From the Dragon's Mouth

John Blankenship, CDR, USN
Chief, Joint OPSEC Support Element



As I was thinking about what might be an inspiring kick-off message for the latest issue of The Purple Dragon, my cell phone beckoned me with its various notification sounds to let me know I had new Facebook posts to read, email to view and calendar reminders. Without thinking, I tapped the icons on the screen to open up the various apps that allow me unprecedented access to the online world and all the information that is ready for my inquiring mind. I casually posted a recent travel photo on a social media site I noticed that the picture was taking an exceptionally long time to upload. I tapped the settings icon to double check my WI-FI connection thinking that I may have inadvertently connected to the store a few doors down instead of the local coffee shop where I was enjoying a highly caffeinated brew to keep me motivated for the rest of the morning. Instead of displaying the name of the local coffee shops wireless connection, I was connected to *cyberhacker22*! Hmmm, maybe I'm not quite as careful or aware as I should be when it comes to connecting with the outside world or keeping my personally identifiable information (PII) safe. Remember……they are always watching you. Stay vigilant!

Is there something *YOU* want to see in the next Purple Dragon?

OPSEC Questions?

Real-life OPSEC successes?

Let us know!

Joint Information Operations Warfare Center

Joint OPSEC Support Element (JOSE)

2 Hall Blvd, Suite 217

JBSA LACKLAND, TX 78236-7074

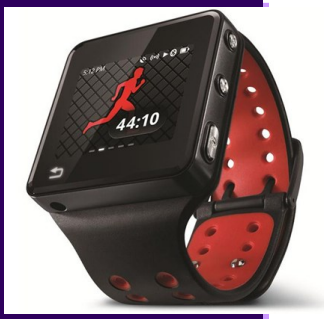
Editorial Staff – Email: jiowc.jose@us.af.mil

Phone: (210) 977-5192 DSN 969-5192

http://www.facebook.com/JIOWC.OPSEC.Support

OPSEC & the Modern Fitness World

Mr. Tomas Ovalle
Joint OPSEC Support Element



"Step back and take a look at what these devices may reveal about you."

We have all probably seen one in our office or in our lunch areas. We may even be one of those wearing these new fitness devices: wearable tech-gear that tracks your movements and provides day-by-day updates on your overall activity and goals. These devices are linked to our phones and our lifestyles. They come by many names such as Fitbit, Nike+ FuelBand, and Jawbone UP to name a few. Similar fitness trackers have exploded in popularity in the last year or so. And they're just getting started according to research firm Canalys. In 2014, 8 million "smart" activity-tracking wristbands are expected to ship, and sales figures predict that number will reach 23 million units by 2015 and more than 45 million by 2017.

As an OPSEC professional or security minded individual, should you be concerned? What is wrong with people taking advantage of the latest technology to stay in shape and live an active lifestyle? There is nothing wrong with it as long as you pause, step back and take a look at what these devices may reveal about you, your lifestyle and work activities. Remember, these devices, when linked to an online account, can in fact track your movements via GPS. What about third party applications that cater to these devices? Who generates those apps? Could they possibly be sponsored by government adversaries seeking to capitalize on a potential vulnerability?

Knowing the inherent risks of any devices, especially emerging technologies, can be a challenge especially for security managers who must weigh any potential vulnerabilities. Does the device have Bluetooth capability? Does it have WiFi connection? Can the device be introduced into a SCIF? Do unit policies address these emerging technologies?

Let's say for example you have one of these devices that's linked to an online account that allows you to access your fitness goals and achievements. Your account may even be linked to online maps that plot every route or trail you use via GPS. What if your account is hacked and an adversary, even a criminal, wants to know your whereabouts? Could this technology be used against you or against our forces?

As members supporting the military, it's not uncommon to deploy to locations downrange. What if you take your fitness devices with you in order to continue staying in shape? What could we reveal about ourselves? TDY locations? Duration of deployments? Are you home and can you be a target of opportunity for random crime/home invasion?

Technology, for all their advantages, can carry inherent risks. OPSEC is all about risk mitigation and vulnerability awareness.

Stay Fit, Stay Safe!

Upcoming Training Dates:

OPSE-2500
20-23 October; San Antonio, TX

OPSE-1500
19 October; San Antonio, TX
27 October; Fort Belvoir, VA

OPSE-2380
20-21 October; Tampa, FL
16-17 November; Humbert Field, FL

https://www.iad.gov/ioss

JIOWC OPSEC SUPPORT

JIOWC.OPSEC.Support

www.dvidshub.net/unit/JIOWC
www.youtube.com/user/JointOPSECSupport

Real–World OPSEC "Ooops!"

LCDR Kurt Fischl
Joint OPSEC Support Element

It is usually not a good idea to tell the enemy where you are and how you are coming to get them. A recent article published by Vice News correspondent David Cenciotti detailed how a possible US Special operations mission was tracked using nothing more than the internet. The culprit it would seem is the ADS-B transponder. ADS-B or Automatic dependent surveillance-broadcast is a cooperative surveillance technology in which aircraft determines position via satellite navigation and broadcasts it enabling air traffic ground stations and other aircraft to receive the information. The system works similarly to the maritime AIS system.

Websites such as Flightaware.com and Flightradar24.com use this information to track and display aircraft in near real-time enabling any adversary to have a common air picture of cooperative air tracks. Fortunately many times OPSEC measures and countermeasures are easy to implement and free as it is in this case. It would seem reasonable that if you are planning a sensitive mission over potentially hostile territory it would be advisable to turn off your transponder to avoid being tracked by anyone with an internet connection. Stay secure my friends!

"…turn off your transponder to avoid being tracked by anyone with an internet connection"

Recent PII Compromises

- The Defense Pentagon's Joint Staff falls prey to a spear phishing attack affecting some 4,000 users on the defense Department e-mail network, compromising sensitive business and private information.
- The Office of Personnel Management database hack compromised 22.1 million past and present federal employees and their friends and family members, revealing private information and increasing potential of blackmail.
- The IRS Internet tax form service breach exposed the personal information of 100,000 people revealing Social Security information, date of birth, tax filing status, and street addresses.

How Do I…Protect PII?

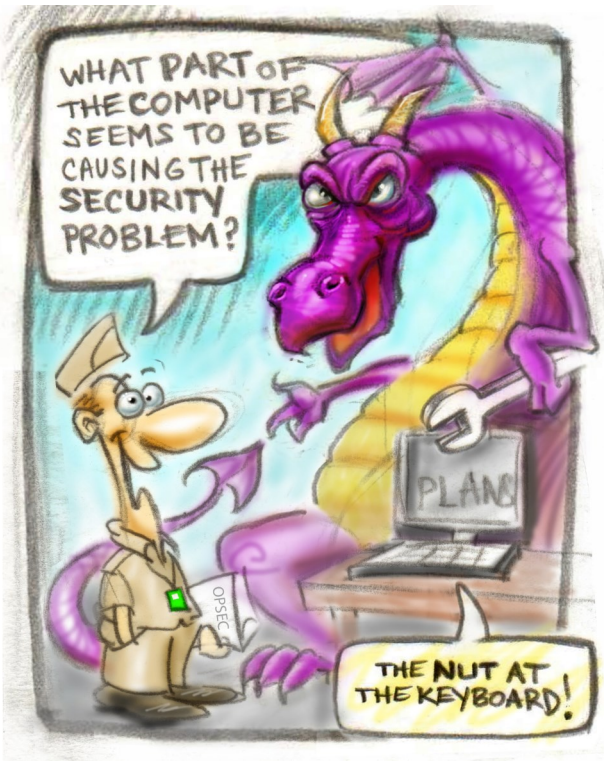
Awareness Training. Ensure everyone has completed unit specific Privacy Training.
Maintain control. Ensure PII is locked, stored, or saved in a secure location from un-authorized access.
Limit to "need-to-know". Ensure only personal with a legitimate purpose has authorized access to PII.
Limit requests for PII. Do not request personal information if it is not required.
Destroy discarded PII. Destroy files beyond reconstruction and/or made unrecognizable.
Label documents. Mark documents with "For Official Use Only (FOUO) - Privacy Sensitive: Any misuse or unauthorized disclosure of this information may result in both criminal and civil penalties." Include a similar label in the subject line.
Cover Sheet. Have a cover sheet for documents containing PII. For example: DD Form 2923 Privacy Act Data Cover Sheet.
Minimize Files. Schedule an annual record disposal to eliminate old PII files.
Sign & Encrypt Emails. Emails containing PII shall be digitally signed & encrypted.

Resources:

AMRDEC SAFE Allows the transfer of up to 25 encrypted file(s), 2 GB each to a .mil or .gov addresses and is authorized for uploading PII files.
https://safe.amrdec.army.mil
White Pages To locate contact information on any member working for DoD to include military, government civilian and government contractors.
https://www.whitepages.mil
DoD 411 To download the required mailbox certificates (to encrypt emails) for the intended recipient. (.mil or .gov)
https://dod411.gds.disa.mil
Military CAC At home residence computer CAC Reader install steps.
http://www.militarycac.com

FROM "HALLS AND WALLS" TO THE "BIG BOY TABLE"

Ms. Jessica O'Dell
Joint OPSEC Support Element



How many of you Purple Dragons out there have OPSEC experience but lack Planning experience? How many of you out there are Planners with little to no OPSEC experience? Neither of you are alone. Did you know that the demand right now for OPSEC *Planners* is VERY HIGH but the supply is LOW, due to the fact that very few professionals have both skillsets? If this sounds like you, know that there's a course that can fix that for you, and make you HIGHLY marketable to boot! It's called the Defense OPSEC Planner's Course, or DOPC (dop-see), and folks…YOU WANT THIS COURSE!

In 2012, a DOD Education and Training Needs Assessment (ETNA) team discovered that, " (U) Current CCMD OPSEC Programs focus almost exclusively on programmatics: HQ and facility 'halls and walls' training programs, regulatory/ administrative compliance… [and lack] a more holistic understanding and demand signal for the application of the doctrinal OPSEC process across the range of military operations."

The DOPC course teaches you not only how to do this, but also equips you with "Ops Speak," the language necessary to communicate to other operational planners. And guess what? It's highly hands-on (no 'death by PowerPoint' here), and it only costs your unit five days. Imagine…five days can change your entire professional profile. Instead of being another face in the crowd, you'll be at the "big boy table" having real world effects on Operations and Plans. So why haven't you registered yet?

The schedule, description, registration and application information for DOPC can be found at:

http://jfsc.ndu.edu/Academics/JointC2InformationOperationsSchool(JC2IOS)/InformationOperationsDivision.aspx