The Purple Dragon

Volume 28 Winter 2015

From the Dragon's Mouth

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

While watching the latest presidential debates I started thinking about what changes the next election will bring. If you read any newspaper, watch any television or follow any social media sites you will have various sources relentlessly attempting to persuade you to think a certain way, support a certain candidate and vilify all other contestants in the race. While we enjoy the right and responsibility to cast our ballot for whichever candidate we believe will best represent our interests as an individual, we must be careful what we post on social media because it just might come back to haunt you. For example, when you were younger, you may have been passionate about your right to have neon multi-colored hair because you wanted to express your individuality. Maybe you called everyone who didn't agree with you stupid on your neon hair activist blog. Several years later, you apply for a management position at a company (your hair is just one color now). The HR department does an open source search on you like most companies do and stumble upon your blog. The VP of the division where you are applying just happens to have been the same "jerk" that wouldn't support your assertion that your neon multi-colored hair was A-Okay for the workplace. Not surprisingly, the company decides you may not be a "good fit" for the job. What happened? That was years ago and you've changed, you were young, didn't know any better! Things you post on the internet stay there forever. You can't ever really hide it and you can't get it back. Be careful what you post. What you think right now might not be what you think in 5 years.....or in 5 minutes. Stay vigilant my friend!

Inside this issue:

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

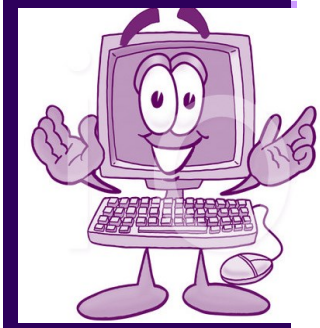
Editorial Staff – Email: jiowc.jose@us.af.mil

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

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

OPSEC & Your Home Network

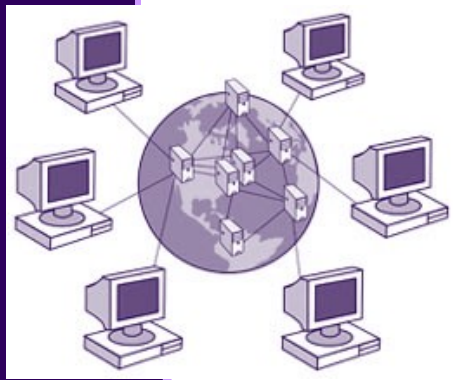
LT David Grimaldo & Mr. James Chavez
Joint OPSEC Support Element



"Your home network, especially if wireless, is vulnerable because of its default configuration."

The adversary desires the unclassified information you possess. Your home network, especially if wireless, is vulnerable because of its default configuration. That is to say, you can often connect immediately to the Internet without additional configuration and is frequently used it to conduct personal and official government business. (eg training, DTS, etc) Also, you may be unwilling to add configuration safeguards because it seems too difficult or are reluctant to spend the time. This is what the adversary wants to happen. Routers are directly accessible from the Internet and are easily discoverable, continuously powered at maximum output, and frequently vulnerable because of their default configuration. Such as, default usernames and passwords, and default SSID.

NOTE: A service set identifier (SSID) is a unique name that identifies a particular wireless local area network (WLAN) that can typically identify the manufacturer or device.



Fundamental Practices to reduce your vulnerability:

- *When possible consider using a physical connection*
- *Change the default username and password often (90 days)*
- *Change the default SSID*
- *Disable SSID broadcast*
- *Don't stay logged in to the management website for your router*
- *Turn the network off when not in use*
- *Frequently update router firmware and patches*

Advanced Practices to reduce your vulnerability:

Configure Wi-Fi Protected Access 2 (WPA2)-Advanced Encryption Standard (AES) for data confidentiality. Wired Equivalent Privacy (WEP) is not recommended. If your router or device supports only WEP, but not other encryption standards, you should upgrade your network device.
NOTE: WPA2 incorporates the Advanced Encryption Standard (AES) 128-bit encryption that is encouraged by the National Institute of Standards and Technology (NIST). WPA2 with AES is the most secure router configuration for home use.

Immediately disable WPS. A design flaw that exists in the Wi-Fi Protected Setup (WPS) specification for the PIN authentication significantly reduces the time required to obtain the entire PIN because it allows an attacker to know when the first half of the 8-digit PIN is correct after a certain number of failed attempts to guess the PIN.

Limit WLAN signal emissions. WLAN signals frequently broadcast beyond the perimeters of your home or organization, allowing eavesdropping by intruders outside your network perimeter. Therefore, it's important to consider antenna placement, antenna type, and transmission power levels. A centrally located, omnidirectional antenna is the most common type used. If possible, use a directional antenna to restrict WLAN coverage to only the areas needed. Experimenting with transmission levels and signal strength will also allow you to better control WLAN coverage. NOTE: A sensitive antenna may pick up signals from further away than expected and a motivated attacker may still be able to reach an access point that has limited coverage.

Disable UPnP when not needed. Universal Plug and Play (UPnP) is a handy feature allowing networked devices to seamlessly discover and establish communication with each other on the network. Though the UPnP feature eases initial network configuration, it is also a security hazard allowing malware within your network to use UPnP to open a hole in your router firewall and let intruders in.

Disable remote management. Disable this to keep intruders from establishing a connection with the router and its configuration through the wide area network (WAN) interface.

Monitor for unknown device connections. Use your router's management website to determine if any unauthorized devices have joined or attempted to join your network. If an unknown device is identified, a firewall or media access control (MAC) filtering rule can be applied on the router.

Is Your Smart TV Tracking Your Activities? Dumb It Down!

Mr. James Chavez
Joint OPSEC Support Element

Smart TVs regardless of the manufacturer are tracking your Internet-based activities unless you change the default privacy settings.

Black Friday and Cyber Monday sales show millions of Smart TVs sold to consumers who are completely unaware that their new TV is really smart! And the name brand doesn't matter because the marketing industry has effectively partnered with most manufacturers to capture usage data from its consumers.

Smart TVs track what you watch and links that data to your IP address then shares it with third parties. An example is the "Smart Interactivity" feature that is turned on automatically (by default out of the box) on more than 10 million Vizio TVs. Vizio isn't the only TV maker to be a little too smart for its users' own good. Earlier this year, Samsung Smart TV privacy policy states it captures voice commands, text and other usage data from its customers.

OPSEC Analysis:

It's no secret that your data is targeted by cyber criminals that includes nation state and other foreign intelligence entities. Therefore, you as a warfighter with access to sensitive unclassified and classified information need to be extra vigilant of potential vulnerabilities and aim to improve the cybersecurity culture of not only yourself but that of your peers, subordinates and leaders. Your individual human performance when it comes to cybersecurity awareness demands personal as well as professional (on-the-job) enhancement. Take the initiative and think about potential vulnerabilities posed to you and your organization, regardless if indirectly or directly.

OPSEC Recommendation:

Be smart.... search online for your particular Smart TV user manual and following the instructions on *how-to-disable* or *disable* the automatic content recognition feature on your Smart TV.

"Smart TVs track what you watch and links that data to your IP address then shares it with third parties."

Best Practices on Traveling With Your Smartphone

Before DEPARTURE

- ❑**Save** all important data
- ❑**Fortify** passwords
- ❑**Update** software and apps
- ❑**Encrypt sensitive** files
- ❑**Delete** sensitive information
- ❑**Enable** screen lock and timeout
- ❑**Enable** Firewalls
- ❑**Disable** Bluetooth and GPS
- ❑**Leave** nonessential devices at home

During TRAVEL

- ❑**Maintain** physical control always
- ❑**Terminate** connections after Wi-Fi use
- ❑**Use** a VPN
- ❑**Visit** secure websites only
- ❑**Disable** file sharing
- ❑**Avoid** public Wi-Fi networks
- ❑**Never** use "remember me" for passwords
- ❑**Don't** click links in text or email messages
- ❑**Don't** download apps
- ❑**Don't** connect to unknown devices

After RETURN

- ❑**Avoid** immediately connecting device to personal or business networks
- ❑**Scan** devices for malware independently or through your organization
- ❑**Change** all passwords

New Navy OPSEC App!

(As seen in NavyTimes)

OPSEC violations are only a few thumb taps away. And now, so is guidance about how to avoid them.

In December, the Navy released an app designed as a one-stop shop for all things operations security. Topics range from cautions against using geotagging on your smart phone to age-old threats like an eavesdropping server.

"Naval OPSEC" is the Navy's fifth mobile application and can be downloaded on Apple iTunes and Google Play. You can quickly review and complete your requirement for OPSEC General Military Training on the app.

OPSEC BOLO: Revised OPSEC Program Managers and Coordinators Course for Joint OPSEC Practitioners

Mr. John Garbelotti
Joint OPSEC Support Element

Coming soon to a classroom near you will be the Defense OPSEC Coordinators (DOCC-2480) and Defense OPSEC Managers (DOMC-2490) courses. These will replace the OPSE-2500 course and are equivalent to the Interagency OPSEC Support Staff's OPSE-2380 and OPSE-2390, but will include joint doctrine discussions. This three day course is divided into two major blocks of instruction.

The first day-and-a-half is the DOCC-2480 and will focus on the 5-step OPSEC process and the duties and responsibilities of OPSEC coordinators and OPSEC working group members. The highlight of this portion of the course is a practical exercise which allows the student to get dirty applying OPSEC. Completing this first block (DOCC-2480) provides training for OPSEC coordinators and working group members, and can also be taught as a standalone course for this purpose.

OPSEC Program mangers will receive additional training during the remaining day and a half with the presentation of DOMC-2490. Instruction includes OSPEC program management, OPSEC and contracting, OPSEC assessments, an intro to OPSEC planning, and OPSEC in exercises. While the focus of this course (DOMC-2490) is to train joint-level OPSEC program managers, the course is equivalent to the IOSS's Program Managers courses (OPSE-2380&2390), meeting both DoD and service OPSEC Program Manager requirements.

The schedule and registration for future courses can be found as always on the IOSS' website: https://www.iad.gov/ioss. Contact the JOSE with any questions you may have. We look forward to seeing you in class!

Upcoming Training Dates:

OPSE-1500
4 March; Yokota, Japan
18 March; Peterson AFB, CO

DOCC-2480/DOMC-2490
1-3 March; Yokota, Japan
8-10 March; Honolulu, HI
15-17 March; Peterson AFB, CO

OPSE-2380
16-17 March; Linthicum, MD
11-12 April; Norfolk, VA
12-13 April; Tampa, FL

https://www.iad.gov/ioss