Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

The Weekly Newsletter of The George Washington University Cyber Security Policy and Research Institute

Quick Links

About CSPRI

Contact Us

Newsletter Archive

Blog: The CSPRI Byte

Follow Us

Follow us on Twitter:
@gwCSPRI

Follow CSPRI Director, Lance Hoffman:
@lancehoffman1

Follow CSPRI Associate Director, Costis Toregas:
@DrCostisToregas

August 24, 2015

Eleven (11) events scheduled in the Greater Washington Area in the next few weeks.

Cyber Security Policy News

Ashley Madison hackers release user data

-A hacking group that last month broke into AshleyMadison.com, a Web site with 37 million users and geared toward helping married people set up extramarital affairs -- made good on its threat to release the company's user database. And as the National Journal reports, the release of that data is more than just an act of public shaming: It's a real security threat. "With the information made public, hackers can and likely will leverage the database to get into other password-protected sites and systems," writes Kaveh Waddell. "And since the *Ashley Madison*data dump also included thousands of government email addresses, criminals now have access to personal information about military and intelligence officials."

Ashley Madison leak: What this could mean for military personnel

Indeed, the Secretary of Defense took to the podium last week and to say that the Department of Defense is investigating the leak, which reportedly included the email addresses of more than 10,000 military service personnel. "I'm aware of it, of course it's an issue, because conduct is very important," Carter told reporters at the briefing, The Hill reported. The publication notes that adultery in the military is a prosecuteable offense under Article 134 of the

Events

August 26
ISSA Baltimore: Business Continuity

August 27
CharmSec Meetup

September 1
Mid-Atlantic Security Conference

September 2-3
Safeguarding Health Information

September 9-10
Intelligence and National Security Summit

September 9-11
2015 Cybersecurity Innovation Forum

September 10
Managing Cyber Risk and the Role of Insurance

September 10
Cyber 6.0

September 10
Senior Executive Cyber Security Conference

Uniform Code of Military Justice. Maximum punishment includes dishonorable discharge, forfeiture of all pay and allowances, and confinement for one year. As such, Carter told reporters that service members found to have used adultery website Ashley Madison could face disciplinary action.

New reports indicate that hackers are already leveraging the leaked AshleyMadison data to conduct extortion attacks. Experts say it is very likely that cyberattackers will leverage the AshleyMadison data to make it easier to deliver malicious software and phishing campaigns. Tom Kellerman, chief cybersecurity officer at Trend Micro, said attacks against military personnel who used AshleyMadison may well target spouses of people whose information is included in the database - all in a bid to infect the spouse as a way to eventually steal information from the real target (the cheating military husband or wife). "Something must already be going on for [the Secretary of Defense] to actually have a press conference on that," Kellerman said. "We may actually see spear-phishing campaigns against spouses of individuals who are involved in this, attacks that say, 'Hey, your wife or husband was involved in this site, do you want to see proof of that?' And the proof, in this scenario, would be a a booby-trapped attachment that deploys spyware or malware.

Tax refund request scam
-The Internal Revenue Service (IRS) disclosed last week that identity thieves abused a feature on the agency's Web site to pull sensitive data on more than 330,000 potential victims as part of a scheme to file fraudulent tax refund request. According to KrebsOnSecurity.com, the site that first publicized that that ID thieves were abusing the weakness, said the new number from the IRS was three times the previous estimates by the agency. The IRS has taken the problematic "Get Transcript" feature offline, but Krebs says the agency's Web site is still vulnerable: "The IRS has responded to the problem of tax ID theft partly by offering Identity Protection PINs (IP PINs) to affected taxpayers that must be supplied on the following year's tax application before the IRS will accept the return," Krebs writes. "However, the IRS.gov Web site allows consumers who have lost their IP PINs to recover them, and incredibly that feature is still using the same authentication method relied upon by the IRS's flawed Get Transcript function."

Spotify privacy policy controversy
-Music streaming service Spotify raised many an eyebrow last week with the release of a new privacy policy that says the company will access smartphone data including motion sensors, GPS trackers, photos and contacts, and that the company's app can share that information with the company's partners. "This has all been made apparent by a rather significant

September 14-16
EnergySec Security and Compliance

September 16
GW Cyber Academy Open House

Click here for detailed descriptions

update to the Spotify privacy policy, pushed out to users today," writes Thomas Fox-Brewster for Forbes. "Upon opening the Spotify app up this morning, your reporter was greeted with a request to agree to the new conditions. A quick comparison with the previous privacy policy using the Wayback Machine showed some major changes had been made. I'm now considering whether the £10 I pay for a premium membership is worth it, given the amount of privacy I'd be giving away by consenting."

According to The Hill, Spotify apologized to users and backpedaled shortly after the release of the new policy prompted an Internet backlash from users. "The company's chief executive Daniel Ek wrote in a **blog post** that the company would 'ask for your express permission' before accessing any of the data covered by the new terms, including photos, location data, contacts or your device's microphone," writes Mario Trujillo.

About this Newsletter

This newsletter is a weekly summary of events related to cyber security policy and research, with a special focus on developments and events in the Washington, DC area. It is published by the Cyber Security Policy and Research Institute (CSPRI) of the George Washington University. CSPRI is a center for GW and the Washington area that promotes technical research and policy analysis of topics in or related to cybersecurity. More information is available at our website, http://www.cspri.seas.gwu.edu

CSPRI

202 994 5613. cspri@gwu.edu
Tompkins Hall, Suite 106
725 23rd Street NW
Washington DC, DC 20052