PHIL PIEMONTE, MANAGING EDITOR • E-MAIL: PPIEMONTE@1105MEDIA.COM

AUGUST 31, 2015 • VOL. 65, NO. 7

FEDERAL EMPLOYEES NEWS DIGEST

Adultery website poses yet another security threat

FEDERAL EMPLOYEES AND MANAGERS have been traced as users of a highly publicized website designed to facilitate adulterous affairs, according to recent investigative news reports.

AshleyMadison.com—which touts the motto "Life is short. Have an affair."—had its data hacked and subsequently dumped as whole databases that are accessible by even modestly able database users. News organizations subsequently searched the data and found the email addresses of anywhere from 1,500 to 15,000 federal employees and managers among the millions of addresses of users of the website.

While some observers have noted that there is no way to know how many of those email addresses were provided by actual visitors to the site, cyber security experts inside and outside of government are alarmed at what many see as a rising tide of careless use of government computer assets. They say that such carelessness has helped enable a wave of security breaches and other opportunities for foreign powers and terrorist organizations, who—armed with the resulting stolen personal data and access to government databases—can manipulate government employees or threaten acts against the United States.

What's Inside

- CBP hiring officers.....2
- Delays encourage ID theft 3
- Informed Investor 6
- In Brief 7
- Federal Benefits Q&A 7

EXTENT OF THE BREACH

One investigative news report released by the *Associated Press*, for example, turned up a conservative estimate of at least 1,500 federal employees' email addresses from a search of the leaked Ashley Madison data. Other news organizations' examinations of the data put the number of federal employees who registered on the site far higher. Whatever the exact number, the evidence points to a sizable crowd of federal employees participating on a website that on its face creates and stores a great deal of data that could be used by blackmailers, extortionists and terrorists, according to cyber security experts.

AP used expert computer investigators to examine the data dump, but said it is not naming the government subscribers it found because none are elected officials or accused of crimes. However, federal employees detected by those investigators did include a num-

PAGE 2

LEGAL MATTERS

BY MATHEW B. TULLY

Agencies attack feds who make IT systems vulnerable to cyber attacks

WITH THE FINGER-POINTING over the massive data breach at the Office of Personnel Management reaching frantic levels, it may only be a matter of time before federal agencies start hunting for employees who may have made them vulnerable to this or other cyber attacks.

Former OPM Director Katherine Archuleta's testimony before the House Oversight Committee, in which she said the only people to blame for the devastating hack were the "perpetrators," should not be viewed as affording federal employees blanket coverage against allegations of cyber security policy violations.

Indeed, blame is like air in the federal government; the system suffocates without it. And if an employee cannot be blamed for this data breach, then agencies will have little problem finding others to blame for smaller breaches.

Violations of cyber security procedures are nothing new in the federal government. Employees caught sharing passwords or using data and information systems without authorization will face an uphill battle at the Merit Systems Protection Board against any adverse action proposals.

Such violations commonly fetch removal notices. That was what happened in *Rene Whittaker v. Internal Revenue Service* (2012), where the agency removed the appellant for

PAGE 8

PAGE 1

ber of feds in critical positions in the government, and hundreds of transactions were associated with Defense Department networks.

Although experts say it is obvious that all online interaction with commercial websites carries some risk of inviting viruses, Trojans and other means for criminals to hack into government databases, and that at present there is no clear dividing line that can be enforced. In fact, federal agencies vary on policies regarding employee use of official computers and Internet access for personal business, including "dating sites"—a fact that some experts say must change if federal agencies are to secure their data.

EXPERTS WEIGH IN

Even if federal agencies aren't in agreement on how stringently they need to press employees to stay out of the murkier end of the web on government networks—or at least how stringently they need to enforce such rules—many experts agree that government workplaces and government networks are endangered by leisure web-surfing, particularly when the surfing involves novelty and dating sites.

Not only do such sites often aggressively market using technology that can be disruptive to electronic tools at work, but they also they invite employees to share information that, if breached, can be used for blackmail purposes.

"This [Ashley Madison] situation sends a clear message that employees at federal agencies should not use government computers, email addresses or networks in connection with any kind of dating—or other personal—activities," James Scott, a cyber security expert with the Institute for Critical Infrastructure Technology, told *FEND*. Scott added that if all federal agencies harmonized their policies to prevent risky uses of their networks—and enforced such rules—it could be a very helpful step in protecting infrastructure from breaches and malware.

"If someone wants to do this kind of thing—dating sites and other leisure activities—they should use a private network, a personal email and possibly some kind of encryption," Scott said.

Scott notes that the marketing emails sent out by such sites—or any commercial site—can contain malware and "phishing" elements that could damage or steal data from federal networks. Other experts agree.

"This website and its data carries real risk, it's a point of pressure," Jacob Furst, a cyber security expert and professor with DePaul University's College of Computing and Digital Media, told *FEND*. "The whole point—or a main point—of doing background checks is to find out if there are pressure points in people's lives—and to keep those from causing security problems. The Ashley Madison site and its data breach definitely could expose—and allow the exploitation of—such points of pressure."

"The Internet isn't secure," Furst said bluntly. "The only way to manage these risks is to get unbelievably rigorous controls over what employees can do with their connected machines. But that can hurt productivity, too—there has to be a balance."

Experts, including Furst and Scott, acknowledge that finding such a balance—by limiting the use of online at work, but not letting that alienate employees or slow work down, and also

PAGE 3

CBP hiring officers

CUSTOMS AND BORDER PROTECTION wants to hire CBP officers at nine locations in four states.

CBP announced Aug. 25 that it is accepting applications for officers to fill positions in Douglas, Lukeville and Nogales in Arizona; Calexico and San Ysidro in California; Pembina and Portal in North Dakota; and Laredo and Presidio in Texas.

Due to mission critical needs, the agency said it is offering a student loan repayment or recruitment incentive for the slots in Lukeville, Ariz.; Portal, N.D; and Presidio, Texas. CBP said incentive applies only to new federal employees and depends on the availability of funds.

According to CBP, the student loan repayment covers $10,000 per year for three years for federally-ensured student loans. The recruitment incentives pay 25 percent of an employee's base pay, including locality pay, per year for three years. The agency requires a service agreement before beginning duty.

An applicant for an officer position must be a U.S. citizen and have been a U.S. resident for the past three years, as well as be referred for selection prior to his or her 37th birthday, or be a preference eligible veteran, or have prior civilian federal law enforcement experience. Applicants also must have a valid driver's license.

Applicants need to pass entrance and medical exams, a drug test, physical fitness assessments, and a video-based test and/or structured interview. Officer candidates also must clear a background investigation and polygraph.

See more at: *www.cbp.gov/careers*.

PAGE 2

by limiting the availability of some databases, but making sure needed information is available—will be very, very difficult.

"It is a real problem—and it's gotten more complicated with people bringing their own devices, their own cell phones to work," Furst said. "And you can put in draconian controls, but when it comes down to it, you have to look at what's the gain and what's the cost."

"Ashley Madison is interesting—overall, I think the OPM breach is a much more serious concern for our government, but this one is not trivial," said Furst, who in recent months has warned that the OPM breach will be causing security concerns "possibly for the next 30 years."

USE OTHER MEANS

"I don't think there is anything you can do about the basic problem here through technology," Furst said. "It's a user issue, not a technology issue. People need to understand—if you use the Internet, it's public. If you don't want it to be public, use another means."

Austen Givens, an expert on cyber security at Utica College who does research on federal data breaches, amplified his colleagues' warnings.

"In fact, the news about Ashley Madison could be a good reminder for federal employees and others to use discretion in terms of what they create and transmit electronically," Givens told *FEND*.

"The bottom line is that absolutely no database that is connected to the Internet is ever truly safe," Givens said. "Despite all the technical prowess and know-how we possess, there are always going to be vulnerabilities. Flawed human beings who are prone to making mistakes build all the tools that we use to protect these databases—and a connection to the Internet means they can possibly be breached."

As for personal security, Givens was equally direct.

"If you are using producing or using anything that's generating any kind of data trail, you should have the assumption that any of it can appear on the front page of the newspaper or on a news page," he said.

And, regarding the security of work product, Givens warned that "you really should assume anything could be breached. If there's something sensitive to communicate to a colleague, it might be worth picking up the phone—or even writing it down on a piece of paper."

Regarding messages from unfamiliar email addresses and other online messages or ads, Givens offers one last piece of advice: "When in doubt—when in doubt, at all—don't click on it!"

"People need to understand—if you use the Internet, it's public. If you don't want it to be public, use another means."

- JACOB FURST, DEPAUL UNIVERSITY

Senators: Processing delays could lead to ID theft

THE LEADERS OF THE SENATE FINANCE COMMITTEE are pressing the organizations that process federal payrolls to speed the processing of tax forms for federal employees in order to head off identity theft and tax fraud.

Sens. Orrin Hatch (R-Utah) and Ron Wyden (D-Ore.), the chairman and ranking member of the committee, respectively, in a letter to the four major federal payroll accounting service centers said that information the lawmakers have gathered indicates that current slow processing times and other inefficiencies at the pay centers are opening up opportunities for identity thieves.

Many identity thieves take advantage of a slow-moving bureaucracy to file counterfeit tax forms—such as W-2s—as part of their schemes to receive inflated or fictitious tax refunds.

"There are over 4.1 million federal employees in the United States, most residing and filing state income tax returns on employment income in 41 of the 50 states and the District of Columbia," the lawmakers wrote. "Unfortunately, state tax administrators are increasingly concerned that the federal government does an inadequate job of filing wage and withholding information with state tax agencies in a complete and timely manner. State tax administrators have reported to us and our staffs that a number of federal agencies routinely fail to file this employee-specific information at all, much less in a timely manner."

"At a time when identity-theft related tax refund fraud has reached epidemic levels, the federal government should be doing all it can to ensure the integrity of the tax administration process, both at the state and federal levels," the letter stated.

The letter went out to the four shared-service accounting centers into which 26 former payroll systems have been consolidated—the Agriculture Department's National Finance Center, the Pentagon's Defense Finance and Accounting Service, the Interior Department's National Business Center; and the General Service Administration's National Payroll Branch.

The letter asks each federal accounting center to report on how efficiently it receives payroll information from agencies, and requests information on how efficient each accounting center is in processing and forwarding federal

PAGE 4

PAGE 3

employee W-2s to the Social Security Administration and state tax agencies.

See the letter at: *http://www.finance.senate.gov/download/?id=F89EC3C6-1145-44CC-94B0-165A6E4F82E5*.

DOJ announces background investigations settlement

A FIRM THAT FORMERLY CONDUCTED federal background investigations has reached a settlement over charges that it had purposely neglected important aspects of its work in order to boost profits, the Justice Department said.

Federal investigators had charged that U.S. Investigations Services, and its parent firm Altegrity, "deliberately circumvented contractually required quality reviews of completed background investigations in order to increase the company's revenues and profits," DOJ said.

According to DOJ, USIS—which provided background investigations services for the Office of Personnel Management under various fieldwork contracts from September 1996 until September 2014—allegedly devised a practice referred to internally as "dumping" or "flushing" that involved releasing cases to OPM and representing them as complete, even though all of the cases allegedly had not received a contractually required quality review.

The allegations, if proven to have taken place, would be illegal under the federal False Claims Act. Under the settlement, the company agreed to forgo more than $30 million in fees, and the federal government dropped its claims that the company is liable under the FCA for the alleged misdeeds.

"Shortcuts taken by any company that we have entrusted to conduct background investigations of future and current federal employees are unacceptable," said Principal Deputy Assistant Attorney General Benjamin C. Mizer, head of the Justice Department's Civil Division.

Altegrity, USIS and their affiliates filed for Chapter 11 bankruptcy protection in February, DOJ noted.

See more at: *www.justice.gov/opa/pr/us-investigations-services-agrees-forego-least-30-million-settle-false-claims-act-allegations*.

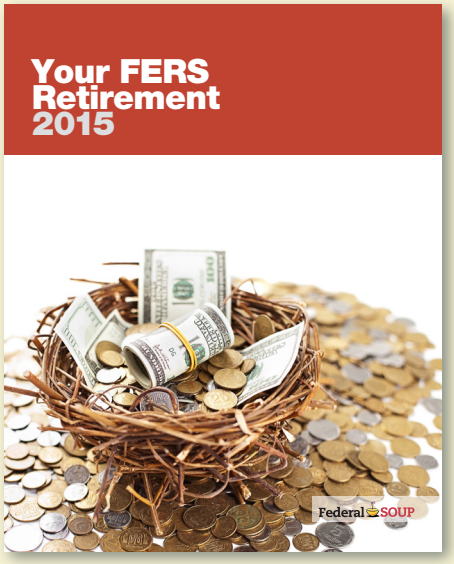
IG says VA employees used unauthorized website

THE DEPARTMENT OF VETERANS AFFAIRS OFFICE OF INSPECTOR GENERAL has criticized thousands of VA employees

PAGE 7

2015 EDITION

Your FERS Retirement



For over 20 years, *Your FERS Retirement* is still the #1 best-selling retirement publication specific to the Federal Employees Retirement System (FERS). Download our latest edition for step-by-step instructions and expert advice on:

- Calculating your basic annuity and adjusting for life changes
- Health insurance (FEHBP) benefits during retirement
- Determining your amount of creditable service
- And more!

Get the retirement you deserve — download *Your FERS Retirement* today!

DOWNLOAD YOUR FREE 2015 EDITION TODAY!

Visit **www.FederalSoup.com/FedStore**.

Federal SOUP
Your Federal Career & Benefits Explained

Informed Investor

SOCIAL SECURITY CELEBRATES 80TH BIRTHDAY: PART II

TO MARK THE 80TH BIRTHDAY of Social Security this month, Informed Investor has dedicated two columns to answering the most frequently asked questions about Social Security. The first column answered questions about Social Security retirement benefits for individuals. This week's column answers 10 of the most frequently asked questions about Social Security family and survivor benefits.

What are the eligibility rules for Social Security spousal benefits?

To qualify for half of a spouse's Social Security benefit, an individual must be (1) at least 62 years old; or (2) any age and caring for the spouse's child younger than age 16 or a disabled child.

What are the requirements to receive Social Security spousal benefits?

A couple must be married for at least one year for one spouse to receive half of the other spouse's Social Security. The exception to the one-year requirement is when the individual is the parent of the spouse's child. A divorced spouse must have been married 10 years to receive a former spouse's Social Security benefit.

Are CSRS annuitants eligible to receive spousal Social Security benefits?

A married CSRS annuitant will most likely not collect any of the Social Security benefits of a spouse/former spouse or a deceased spouse. This is because any individual receiving a pension based on federal or state government work—such as CSRS—and not covered by Social Security is subject to the Government Pension Offset (GPO). The GPO reduces a spousal or survivor Social Security benefit by two-thirds of the amount of the government pension, most likely reducing the spousal or survivor Social Security benefit to zero.

Can children receive Social Security benefits?

When a parent receives Social Security retirement or disability benefits, the parent's children can receive benefits. Children also can get benefits when a parent dies. The child can be a biological or adopted child or a stepchild. A dependent grandchild also may qualify. To get benefits, the child must be unmarried and (1) younger than age 18; (2) a full-time student no higher than grade 12; or (3) 18 years or older with a disability that started before age 22.

Is there a limit to the amount of monthly benefits family members can receive based on the primary earner's full retirement benefit?

There is a limit as to how much Social Security pays in benefits to family members. The total amount paid cannot exceed 150 percent to 180 percent of the primary earner's full retirement benefit.

Which family members are eligible to receive Social Security survivor benefits?

The following family members are eligible for survivor benefits:

- A widow or widower who must be (1) age 60 or older; (2) age 50 or older if disabled; or (3) any age if the widow or widower is taking care of a child younger than age 16 or a disabled child.
- A divorced widow and widower has the same requirements as a married widow or widower except that the marriage to the deceased must have lasted at least 10 years.
- Unmarried children who must be (1) younger than 18 (or up to age 19 if they are attending elementary or secondary school, full time); or (2) any age and were disabled before age 22 and remain disabled.

What should one do when a family member dies?

When a family member dies, a surviving family member should contact the Social Security Administration as soon as possible. In most cases, the funeral home will report the person's death to SSA. A surviving family member would have to give the funeral director the deceased's Social Security number. Surviving family members would still have to contact SSA to start receiving any survivor benefits, if eligible.

How much do survivors receive in benefits?

Social Security determines survivor benefits as a percentage of the deceased's "primary insurance amount" (PIA) at the time of death. The PIA is determined from a worker's lifetime Social Security earnings.

Who can receive a lump-sum death benefit payment of $255?

Social Security will pay a lump-sum death benefit of $255 to (1) a spouse who was living with the deceased person at the time of death; or (2) a former spouse or a child who in the month of the deceased's death is eligible for a Social Security benefit based on the deceased's earnings record.

Can Social Security payments go to beneficiaries of the deceased's estate?

Beneficiaries of the deceased may have been due a Social Security payment at the time of death. Social Security may pay amounts due to these beneficiaries, whether a family member or a legal representative of the estate. Claimants should use Form SSA-1724 (Claim for Amounts Due in the Case of Deceased Beneficiary) which can be downloaded from *www.socialsecurity.gov*. ■

Edward A. Zurndorfer is a Certified Financial Planner and Enrolled Agent in Silver Spring, MD. He is also a registered representative with FSC Securities Corporation, branch address: 833 Bromley St. - Suite A, Silver Spring, MD 20902. Phone: (301) 681-1652. Securities offered through FSC Securities Corporation, member FINRA/SIPC. EZ Accounting and Financial Services and FSC are independent companies.

Federal Benefits Q&A

QUESTION: "I see they are having open season for life insurance. I will choose an amount five times my salary. Can I reduce the five times salary to say three times salary at any time? Or am I locked in for the five times until I cancel it entirely?"

ANSWER: You will be able reduce your Option B FEGLI coverage from five times your salary to three times your salary at any time using Form SF 2817. ■

Readers are encouraged to ask questions related to general employee benefits—such as CSRS, FERS, the Thrift Savings Plan, tax and estate planning, insurance, Social Security and Medicare—at the "Federal Benefits Q&A" at www.FederalSoup.com.

PAGE 5

for their use of an unauthorized social media forum that potentially compromised security.

The VA OIG found that more than 50,000 employees "improperly used Yammer.com, a web-based collaboration technology, which was not approved or monitored as required by VA policy."

The report that summarized the OIG's findings notes that some in senior leadership gave some employees a "false impression" that the forum had been approved for use.

Nonetheless, the OIG said users were in violation of policy when they "downloaded and shared files, videos, and images, risking malware or viruses spreading quickly from the site." The social media/work collaboration site also "regularly spammed and excessively emailed users," the VA report said.

The report comes at a time when data security vulnerabilities across the federal government are being spotlighted—from the OPM data breaches revealed in June affecting just about all federal employees and retirees, to the current reports of feds' data being compromised in leaks from a website promoting adulterous affairs.

See the report at *www.va.gov/oig/publications/report-summary.asp?id=3568*.

Fed pleads guilty to theft of benefits

A TEXAS BORDER PATROL SUPERVISOR pleaded guilty to stealing his deceased grandmother's Social Security benefits, the Justice Department said Aug, 25.

At the hearing at which he entered the guilty plea, the 54-year-old supervisor admitted that he did not report his grandmother's death to the Social Security Administration in February 2000, and from that time until August 2011 continued to negotiate his grandmother's monthly widow's benefits, which were being deposited into their joint bank account.

The man, who DOJ said illegally collected a total of $108,516 in Social Security benefits, faces up to 10 years in federal prison and a possible $250,000 fine.

DOJ said the case was investigated by the SSA Office of Inspector General, the Department of Homeland Security Office of Inspector General, and the Bureau of Vital Statistics Fraud Unit.

See more at: *www.justice.gov/usao-sdtx/pr/border-patrol-supervisor-guilty-stealing-social-security-benefits*. ■

Thrift Savings Plan Share Prices

Funds	Aug. 26	Month Ago	Year Ago
G Fund	14.8069	14.7784	14.5062
F Fund	16.9208	16.8788	16.5330
C Fund	25.9608	27.7581	26.1941
S Fund	34.9714	37.5357	35.8193
I Fund	24.1455	26.0648	26.4062
Lifecycle Funds			
L Income	17.5322	17.7392	17.3194
L 2020	22.7382	23.5049	22.8354
L 2030	24.4638	25.5665	24.7718
L 2040	25.8882	27.2555	26.3618
L 2050	14.6176	15.5067	14.9906

Register free to get rates of return and other TSP info at: www.FederalSoup.com/pages/resources/thrift-savings-plan.aspx

PAGE 1

inserting a personal flash drive in her government-issued laptop and infecting it with malware. The appellant in *Lenora Porzillo v. Department of Health and Human Services* (2008) received the same penalty for sharing her password with a co-worker and downloading an Excel spreadsheet with the names and Social Security numbers of more than 1,000 employees from a restricted drive so she could send it to her personal e-mail account. And in *Von Muller v. Department of Energy* (2006), the Board found the appellant could be removed for, among other things, attempting to stifle the agency's cyber security measures by "encouraging coworkers to barrage the Cyber Security department with requests to review incoming email attachments."

Probably the best chance for employees facing removal for cyber security policy violations is to show that agency treated similarly situated employees less harshly. Studies have found that 95 percent of cyber security incidents are attributable to human error, and while inadvertent actors account for only 5 percent of the cyber attacker population, IBM claims they are "among the most dangerous."

As stated above, the government often comes down hard on cyber security policy violators, but agencies often fail to do so across the board. I suspect the government's payroll would take a steep hit if that were the case. In *Michelle Washington v. U.S. Postal Service* (2011), for example, an MSPB judge did not sustain the password-sharing specification of an improper conduct charge because "other employees testified that during 'crunch' times this sharing of passwords happened with some frequency to make working more efficient."

In *Smith v. Department of Transportation* (2012), the MSPB and Equal Employment Opportunity Commission refused to sustain the 30-day suspension of an employee for the unauthorized disclosure of government information after the agency refused to provide requested information on how it disciplined similarly situated employees. That failure enabled the EEOC to draw an adverse inference and prove the suspension was retaliation for prior Equal Employment Opportunity activity.

Probably the best chance for employees facing removal for cyber security policy violations is to show that agency treated similarly situated employees less harshly.

Mistakes happen, especially when computers are involved. Federal employees facing removal or suspension for misusing government equipment or violating cyber security policies should immediately consult with an experienced federal employment law attorney. ■

Mathew B. Tully is the founding partner of Tully Rinckey PLLC. He concentrates his practice on representing military personnel and federal employees and can be reached at mtully@fedattorney.com. To schedule a meeting with one of the firm's federal employment law attorneys call 202-787-1900. The information in this column is not intended as legal advice.

SUBSCRIPTION INFORMATION

(800) 989-3363, M-F, 5 a.m.-5 p.m. PT

customerservice@federalsoup.com

Site license assistance:
sitelicense@federalsoup.com

Federal Employees News Digest is included as part of a Federal Soup subscription. 1 year - $39

Published weekly except first week in January and last week in December, 50 issues per year.
Reprints: (212) 221-9595 or
1105reprints@parsintl.com

Federal Tax ID 20-4583700 DUNS #612031414

PUBLISHED BY 1105 PUBLIC SECTOR MEDIA GROUP

Henry Allain, President
Anne Armstrong, Co-President

1105 Media, Inc.
Rajeev Kapur, CEO
www.1105media.com

STAFF

Kristi Dougherty	General Manager
Phil Piemonte	Managing Editor
Sherkiya Wedgeworth	Online Managing Editor
Becky Fenton	Audience Development Director
Mary Keenan	Media Sales Consultant

CONTRIBUTORS:
Nathan Abse, Mike Causey, Mathew B. Tully, Edward A. Zurndorfer, Linda Brooks Rix