ISSA™
Information Systems Security Association
The Global Voice of Information Security

Kansas City ISSA Newsletter

February 22, 2018

Topic: Beyond Password Management: Seven Steps to an Effective Privilege Program

Cyber Ark

Lidia's Italy Restaurant

Inside this issue:

Volume 53, Issue 1 February 2018

The President's Corner

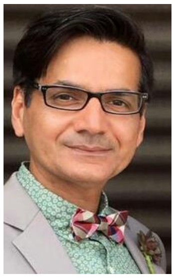
Hello ISSA Kansas City Members and Happy February!

Hope you enjoyed the January presentation on "Cyber Security trends for 2018" by Mike Tyk with Novacoast. I found the topic perfect to kick off our first meeting of the year. If you did not get a copy of the presentation, please reach out to us.

Keyaan Williams is the current President of ISSA International Board of Directors. The ISSA international organization is working on completing a major transition from ISSA's traditional reliance on management companies to a new operating model. Upon completion of the transition ISSA will be able to provide greater transparency, inclusiveness, and value to its members. These changes are progressing slowly as part of the overall transformation of the association. If you have any questions please do reach out. The ISSA International HQ is now located at:

Information Systems Security Association, Inc.
4008 Louetta Road #261
Spring, TX. 77388

If you have questions concerning the Kansas City Local chapter contact me.



Sincerely,

Naeem Babri

President, ISSA Kansas City

facebook Linkedin twitter

Upcoming ISSA-KC Monthly Chapter Meeting Schedule

February 22, 2018 **Beyond Password Management** Cyber Ark Lidia's Italy, Kansas City, MO	March 22, 2018 **Zero Trust Security Architecture** Critical Security Brio's, Kansas City, MO	April 26, 2018 **Topic: Pending** Est-Grp Hereford House, Leawood, KS.

ISSA KC January 2018 Meeting Recap

Cyber Security Trends for 2018

On January 25, 2018, the ISSA-KC Chapter members and other security professionals held a meeting at Hereford House restaurant to network and attend the monthly chapter meeting, on the topic "Cyber Security Trends for 2018". We're getting off the year with a BLAST! There were 42 attendees.

Mike Tykwith Novacoast discussed how our world is networked together, where companies and home users rely on networked systems and the data stored in them. 2018 will be a tipping point year as we all become more connected and influenced by new digital transformations. Mike discussed how the security professional will be presented with new cybersecurity threats and landscapes. He emphasized that cybersecurity is one of the most critical issues that will needed to be addressed, not just in the workplace but in our homes as well.

CONGRATULATIONS TO THE WINNERS! - Brandon Dalpe and Eric Hershberger each won a $25.00 gift card from Novacoast, and Kip Ballinger won ISSA's $50.00 Visa gift card give-away.

Security & Privacy Articles and News

File Your Taxes Before Scammers Do It for You

Author: Brian Krebs, Krebson Security, January 29, 2018
https://krebsonsecurity.com/2018/01/file-your-taxes-before-scammers-do-it-for-you/

Jan. 29, is officially the first day of the 2018 tax-filing season, also known as the day fraudsters start requesting phony tax refunds in the names of identity theft victims. Want to minimize the chances of getting hit by tax refund fraud this year?

File your taxes before the bad guys can! Tax refund fraud affects hundreds of thousands, if not millions, of U.S. citizens annually. Victims usually first learn of the crime after having their returns rejected because scammers beat them to it. Even those who are not required to file a return can be victims of refund fraud, as can those who are not actually due a refund from the IRS

According to the IRS, consumer complaints over tax refund fraud have been declining steadily over the years as the IRS and states enact more stringent measures for screening potentially fraudulent applications. If you file your taxes electronically and the return is rejected, and if you were the victim of identity theft (e.g., if your Social Security number and other information was leaked in the Equifax breach last year), you should submit an Identity Theft Affidavit (Form 14039). The IRS advises that if you suspect you are a victim of identity theft, continue to pay your taxes and file your tax return, even if you must do so by paper. If the IRS believes you were likely the victim of tax refund fraud in the previous tax year they will likely send you a special filing PIN that needs to be entered along with this year's return before the filing will be accepted by the IRS electronically. This year marks the third out of the last five that I've received one of these PINs from the IRS. Of course, filing your taxes early to beat the fraudsters requires one to have all of the tax forms needed to do so. As a sole proprietor, this is a great challenge because many companies take their sweet time sending out 1099 forms and such (even though they're required to do so by Jan. 31).

A great many companies are now turning to online services to deliver tax forms to contractors, employees and others. For example, I have received several notices via email regarding the availability of 1099 forms online; most say they are sending the forms in snail mail, but that if I need them sooner I can get them online if I just create an account or enter some personal information at some third-party site. Having seen how so many of these sites handle personal information, I'm not terribly interested in volunteering more of it. According to Bankrate, taxpayers can still file their returns even if they don't yet have all of their 1099s — as long as you have the correct information about how much you earned. "Unlike a W-2, you generally don't have to attach 1099s to your tax return," Bankrate explains. "They are just issued so you'll know how much to report, with copies going to the IRS so return processors can double-check your entries. As long as you have the correct information, you can put it on your tax form without having the statement in hand." In past tax years, identity thieves have used data gleaned from a variety of third-party and government Web sites to file phony tax refund requests — including from the IRS itself! One of their perennial favorites was the IRS's Get Transcript service, which previously had fairly lax authentication measures.

After hundreds of thousands of taxpayers had their tax data accessed through the online tool, the IRS took it offline for a bit and then brought it back online but requiring a host of new data elements. But many of those elements — such as your personal account number from a credit card, mortgage, home equity loan, home equity line of credit or car loan — can be gathered from multiple locations online with almost no authentication. For example, earlier this week I heard from Jason, a longtime reader who was shocked at how little information was required to get a copy of his 2017 mortgage interest statement from his former lender. "I called our old mortgage company (Chase) to retrieve our 1098 from an old loan today," Jason wrote. "After I provided the last four digits of the social security # to their IVR [interactive voice response system] that was enough to validate me to request a fax of the tax form, which would have included sensitive information. I asked for a supervisor who explained to me that it was sufficient to check the SSN last 4 + the caller id phone number to validate the account."

If you've taken my advice and placed a security freeze on your credit file with the major credit bureaus, you don't have to worry about thieves somehow bypassing the security on the IRS's Get Transcript site. That's because the IRS uses Experian to ask a series of knowledge-based authentication questions before an online account can even be created at the IRS's site to access the transcript.

Now, anyone who reads this site regularly should know I've been highly critical of these KBA questions as a means of authentication. But the upshot here is that if you have a freeze in place at Experian (and I sincerely hope you do), Experian won't even be able to ask those questions. Thus, thieves should not be able to create an account in your name at the IRS's site (unless of course thieves manage to successfully request your freeze PIN from Experian's site, in which case all bets are off). While you're getting your taxes in order this filing season, be on guard against fake emails or Web sites that may try to phish your personal or tax data. The IRS stresses that it will never initiate contact with taxpayers about a bill or refund. If you receive a phishing email that spoofs the IRS, consider forwarding it to phishing@irs.gov.

Finally, tax season also is when the phone-based tax scams kick into high gear, with fraudsters threatening taxpayers with arrest, deportation and other penalties if they don't make an immediate payment over the phone. If you care for older parents or relatives, this may be a good time to remind them about these and other phone-based scams.

Google Took Down More than 700,000 Bad Apps in 2017

From a flashlight app that actually stole your money to a fake WhatsApp that millions of people downloaded, it’s been a busy year for Google's security team.

Author, Alfred Ng, CNET, January 30, 2018

Stamping out harmful apps is a never-ending effort for Google, but at least it's getting easier. On Tuesday, the tech giant said it removed more than 700,000 apps from the Google Play store in 2017, up 70 percent from 2016. More than 2 billion Android devices worldwide rely on apps, whether they're for ordering a pizza or trying to catch Pokemon. Despite the useful features apps can bring, they also have the potential to do a lot of damage.

Last April, ESET, a security company, found that a seemingly harmless flashlight app on the Google Play store was actually malware dedicated to stealing your banking information. Avast, an antivirus company, found the same malware across several apps, like in games of Solitaire. Last September, Google had to delete 50 apps that had been downloaded millions of times before the malware was discovered.

Despite these apps managing to slip through the Google marketplace, the company said 99 percent of apps "with abusive contents were identified and rejected before anyone could install them."

Google was able to do that through machine learning designed to weed out apps with inappropriate content, malware and copycats, Andrew Ahn, the Google Play product manager, said in the blog post. The algorithm is able to detect repeat offenders, and developers that try to abuse the system, Ahn said. Google removed 100,000 bad developers in 2017, he added.

The majority of deleted apps were copycats, made by developers trying to milk the success of popular apps. Google said it had taken down more than 250,000 copycat apps in 2017. A fake version of the popular chatting app "WhatsApp" was downloaded at least 1 million times before Google removed it last November.

Google said it's getting better at detecting harmful apps with its new algorithm, noting that it's been able to lower the number of people who end up downloading malware from its store. The company said that with Google Play Protect, which scans your phone, it's been able to reduce the number of potentially harmful apps by ten-fold compared with 2016.

Beware of These Valentine's Day Scams: Protect yourself from these three common cons

Author: Catherine Fredman, Consumer Reports

Scammers want to get close to you on Valentine’s Day—close enough that is, to swipe your credit card number, steal your personal information, and infect your computer with a virus that lets them plunder your address book for future victims.

How do they do this? One of the most common Valentine's Day scams is through impostors in which con artists trick you into believing they are a legitimate business—an online florist, for example, or an e-card website. Others are phishing scams, which use fraudulent websites and fake emails to attempt to steal your personal data, especially passwords and credit card information.
Three of the most common Valentine's Day scams include:

Bogus e-cards. Scammers count on your curiosity to open an electronic greeting card when you see an innocuous subject line such as, "Someone you know just sent you an e-card." Or they circumvent your suspicion by directing you to a website that mimics one of the popular greeting card sites, such as Hallmark, American Greetings, or Paperless Post. When you click on the link to open the card, however, you'll load malware onto your computer that opens the door to endless spam for you and your address book contacts.

Protect yourself by looking for the confirmation code that proves that the card is legitimate. Use your browser to open the website; don't just click on the email link.

Phony package delivery. Scammers piggyback on gifts or flowers that were ordered online by creating phony delivery emails. If you receive an email about a package you didn't send or a delivery you don't expect, don't open it—especially if it asks you to download a form or click to a separate website. Otherwise, the package you receive could be a nasty virus.

If you receive an email delivery confirmation, be sure to verify the delivery with the shipping company on the phone before opening the email. It could be one of many Valentine's Day scams.

Phishing through flowers. Phishing emails try to fool you into revealing credit card and other personal information. Especially effective among Valentine's Day scams are emails claiming to be from a florist: They warn you that the bouquet you ordered can't be delivered unless you log in and re-enter your credit card information. This scam works because it reaches enough people who actually have ordered flowers and are worried that their nosegay might not show up on time. However, what shows up on your next credit card statement won't smell sweet.

Protect yourself by not clicking on the link and certainly don't enter your credit card information. If you have questions about the delivery, call the florist directly.

Share the love on Valentine's Day—just don't share Valentine's Day scams.

ISSA KC 2018 Mentor Program Launch

ISSA Kansas City Chapter Mentor Program in 2018!

The program is designed to formalize relationships between more senior professional individuals in the chapter (Mentors) and the various levels of security professionals seeking entry or moving through the different phases of this profession (Mentees). Since 2018 is the pilot year for this program for our chapter we need your participation to make it successful! The ISSA KC Board of Directors are working aggressively to launch the program. WATCH THE NEWSLETTER FOR UPDATES.

Call for Mentors

Why should I be a mentor?

Contribute to the professional development of the future workforce;
Help build stronger community fabric;
Impart the principles of an experienced security professional;
Gain a broader view of your own community; and
Give something back to the profession!

Mentor Criteria:

Must actively participate and support chapter events
Must be a current or recently retired security practitioner
Must be willing to commit to the Mentoring Program for a specified period of time

How will I be able to sign up?

We will be accepting applications for Mentors throughout the year. If you are interested reach out to Cheryl Cooper for more detail, vp@kc.issa.org . Complete and submit a Mentor application at www.kc.issa.org

ISSA Journal February 2018

ISSA JOURNAL
The Two Faces of Innovation
From Safe and Dumb to Vulnerable and Smart Products and Infrastructure

February 2018

Volume 16 - Issue 2

Feature articles include:

- The Two Faces of Innovation: From Safe and Dumb to Vulnerable Smart Products and Infrastructure | Steven W. Teppler
- Security Incidents and Breaches in the Healthcare Industry: A Case Study in the Lack of Federal and State Coordination | Barry S. Herrin – ISSA member, Metro Atlanta Chapter
- CPU Bugs: Trading Security for Performance: Exploring the causes and long-term impact from the infamous Meltdown and Spectre vulnerabilities | Adrian Sanabria
- Legal Requirements of Notification of Breaches: An Overview | Steve Kirby – ISSA member, Greater Spokane Chapter
- The Post Exploitation Malware Era | Meir Brown

Members: please click on the following Journal issue links for access:
Computer: Bluetoad - PDF; Mobile: ePub - Mobi

Not a member? Read this month's feature article - The Two Faces of Innovation: From Safe and Dumb to Vulnerable Smart Products and Infrastructure - at no charge or Join Now and gain full access to the *ISSA Journal*.

Certification Corner

CISSP® Certified Information Systems Security Professional

ISC2 CISSP Certification 2018 Changes

For those of you with the CISSP certification, or those who are pursuing a CISSP certification, there will be changes in 2018. Effective April 15, 2018, the CISSP exam will be based on a new exam outline, and the domains and their weights will change. The delivery method will change to Computer Adaptive Testing (CAT) that provides fewer questions in less time. There will be 100 to 150 questions, versus the 250 questions that were offered on the linear fixed exam that many of us have taken. The exam will no longer be up to 6 hours to complete, but up to 3 hours, on the average of 2 hours to complete.

For more information on the changes, check out ISC2's web site, https://www.isc2.org/Certifications/CISSP

Contact: Nicole at certification@kc.issa.org

Contact: Mark Waugh, ISSA Education Committee Member For CISSP, 913-636-7900

Chapter Membership Corner

Contact: Wai Cheng, ISSA Director of Membership, Membership KC membership@kc.issa.org

Webinars/Conferences

- SecureWorld Expo, May 9, https://events.secureworldexpo.com/details/kansas-city-ks-2018/
- Interface 2018 is open for registration. The KC tour date is July 12. Other cities and dates available for those outside of KC. Free to attend. http://interfacetour.com/tour/kcm18/
- B-sides KC Security Learning and sharing conference: April 20 – 21. Free to attend, https://www.bsideskc.org/mission/

ISSA-Kansas City February Chapter Event

On February 22, 2018 the ISSA-KC Chapter members, and other security professionals will hold a meeting at Lidia's Italy Restaurant in Kansas City, MO, to network and attend the monthly chapter meeting, with presentation topic.

Speaker: Troy Brueckner is a Certified Information Systems Security Professional (CISSP) with an extensive record of assisting organizations improve network and data confidentiality, integrity, and availability. He joined CyberArk Software, Inc.in 2013 to assist in their mission to "Provide a new layer of security to protect the heart of the enterprise from advanced cyber threats." Prior to CyberArk, he served as Vice President for Infogressive, Inc. and as Security Architect for Alexander Open Systems, Inc. He serves on the Board of Directors for InfraGard Nebraska. Mr. Brueckner is a current member of the FBI Omaha CAAA Board of Trustees and Past President of the (ISC) 2 Omaha-Lincoln Chapter.

Topic: Beyond Password Management: Seven Steps to an Effective Privilege Program

Topic Summary: Management of passwords, keys, and secrets is being addressed within every organization in one way or another (or many), but does your privilege account management program really keep attackers from fulfilling their mission ... or does it just make administration less cumbersome? We will explore the common elements in nearly every high-profile breach and how compromised credentials were necessary to the overall "success" of the attack. More importantly, we will discuss the steps every organization can take to reach an acceptable level of "cyber-hygiene" within their privilege program.

Location: Lidia's Italy Restaurant, 101 W. 22nd street, Kansas City, MO. 64108

Agenda:
11:30 AM - 12:00 PM Greeting and registration
12:00 PM - 1:00 PM - Meeting & Presentation
1:00 PM - 1:30 PM - Questions, Answers & Networking

Menu: Pasta Tasting Trio - A sampling of three daily-made fresh and filled pastas.
Biscotti Platters - An assortment of house-made cookies & sweets to pass and share family style.
Soft drinks, Iced Tea, Coffee

*Vegetarian option available, please note at registration at Brio
* *Menu subject to change. **

Price:
$25.00 for ISSA Members,
$35.00 for Guests/Non-Members
Maximum Reservation: 35

Credit(s): 1 CPE credit

We look forward to seeing you at the event. If you have any questions about the event or how to register, please email our RSVP email, or contact the venue for directions.

Register

The Information Systems Security Association (ISSA) is an international organization providing educational forums, publications and peer interaction opportunities that enhance the knowledge, skills and professionalism. The primary goal of ISSA is to promote management practices that will ensure availability, integrity and confidentiality of organizational resources.

novacoast

CYBERARK

IBM

radware

AOS

CARBON BLACK
ARM YOUR ENDPOINTS

InteliSecure

Integrity
SECURITY | RISK | COMPLIANCE

VARONIS

tenable
network security

CISCO
OpenDNS

viawest

Lockpath

netskope

President
Naeem Babri
president@kc.issa.org

Vice President
Cheryl Cooper
mailto:vp@kc.issa.org

Director of Social Media
Melissa Salazar
socialmedia@kc.issa.org

Secretary of Board
Rochelle Boyd
secretary@kc.issa.org

Newsletter Chief Editor
Cheryl Cooper
newsletter@kc.issa.org

Treasurer
Gary Kretzer
treasurer@kc.issa.org

Director of Membership
Wei Cheng
membership@kc.issa.org

Director of Education
Larry Dilley
certification@kc.issa.org

Director of Programs
Carmen Banks
programs@kc.issa.org

Webmaster
Thomas Badgett
webmaster@kc.issa.org

Director of Events
Dan Boethe
events@kc.issa.org

Past Presidents
Bob Reese
Tom Stripling
Jeff Blackwood
Michelle Moloney