ISSA Information Systems Security Association
Colorado Springs Chapter
WWW.ISSA-COS.ORG

# ISSA-COS NEWSLETTER

VOLUME 9 NUMBER 5 MAY 2020

Colorado Springs, Colorado

## April Was *BUSY!*

### A Note From Our President

By Mr. Ernest Campos

Fellow Members of ISSA-COS,

Wow! If anyone ever tells you going virtual will reduce your workload and give you more free time in your life, don't believe them. It is a lie! Over that last two months, our chapter has been busier than ever! Thankfully, it has all been a good kind of busy. Our chapter has been flourishing with opportunities, partnerships, and events. I am proud of the impact we are making in our community and with businesses across America.

During the month of April, we kicked-off our weekly online series with five (5) Thursday night presentations. Prominent guest speakers included **Mr. Art Cooper, Mr. Wally Magda, Dr. Erik Huffman, Mr. Mark Spencer (ISSA-COS President Emeritus), Mr. Justin Whitehead, Mr. Rob Carson, Mr. Jay Carson, and Mr. Ryan Dozier**. All in one month! We averaged 42 attendees at each presentation and have issued hundreds of CPE/CEU credits. What a great month but, wait, that wasn't all…

Apart from our public events, our chapter negotiated a new strategic partnership with the Info-Tech Research Group. In June, we will reserve a special night to showcase this partnership to all our members. You won't want to miss that event! Also, in April, we kicked-off the planning for our **2020 Peak Cyber Symposium**. This year will be our 10-year Anniversary for this event. Opportunities for Early Bird Registration, a Call for Speakers, and a Call for Sponsors/Exhibitors will open later this month. Lots of great plans are underway to include a live taping of the **New Cyber Frontier** podcast, a **Chamber and EDC** Ribbon Cutting ceremony, and a full-scale job fair sponsored and facilitated by **Cleared Careers**. Oh, and don't forget the "Boss of the NOC" Capture the Flag challenged sponsored and facilitated by **Splunk! and Epoch Concepts**! Like I said earlier… April was a very, busy month.

As we shift into May, our weekly online series will continue with another great schedule of phenomenal speakers. Please register early on our website to attend these events. You will receive valuable information and earn CPE/CEU credits for your time. During the month of May, we will continue

*(Continued on page 4)*

***The ISSA Colorado Springs Newsletter incorporates open source news articles in compliance with USC Title 17, Section 107, Paragraph a (slightly truncated to avoid copyright infringement) as a training method to educate readers on security matters .***

***The views expressed in articles obtained from public sources within this newsletter do not necessarily reflect those of ISSA, this Chapter or its leadership.***

***Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our members, and do not constitute or imply endorsement by ISSA or the Colorado Springs Chapter of ISSA of any entity, event, product, service, or enterprise.***

# FBI Warns of Human Traffickers Luring Victims on Social Networks

By Sergiu Gatlan, BleepingComputer, March 16, 2020

A two-year study reveals the cost of fake passports, compromised bank accounts, and DDoS attacks on the dark web.


FBI's Internet Crime Complaint Center (IC3) today issued a public service announcement on human traffickers' continued usage of online platforms like dating sites and social networks to lure victims.

"The FBI warns the public to remain vigilant of the threat posed by criminals who seek to traffic individuals through force, fraud, or coercion through popular social media and dating platforms," the PSA says.

"Offenders often exploit dating apps and websites to recruit—and later advertise—sex trafficking victims. In addition, offenders are increasingly recruiting labor trafficking victims through what appears to be legitimate job offers."

*"Human trafficking occurs in every area of the country and occurs in many forms..."*

## Online platforms tools used against vulnerable targets

According to the FBI's investigations, victims from various different backgrounds from rural areas to large cities are being lured by human traffickers into forced labor or sex work using online platforms.

In many cases, the criminals will pose as legitimate job recruiters or agents of employment agencies and will bait potential victims with the promise of fake employment and a better life.

Individuals who share personal information on online platforms are the ones most likely to be targeted by such criminals, especially after posting about "financial hardships, their struggles with low self-esteem, or their family problems."

The traffickers will use their targets' stories as the base for well-planned attacks via the Internet, convincing them that they want to be helpful or that they are interested in a relationship.

However, their victims will subsequently be coerced into sex work or forced labor after the traffickers manage to establish a false sense of trust and they persuade them to meet in person.

## Human traffickers using online platforms

During the last few years, the FBI discovered multiple cases of human traffickers using popular social networks and dating sites to recruit victims.

Among the multiple such cases identified over the years, the FBI shares the following three examples:

- In July 2019, a Baltimore, Maryland, man was convicted on two counts of sex trafficking of a minor and one count of using the Internet to promote a business enterprise involving prostitution. The perpetrator targeted two girls after they posted information online about their difficult living and financial situation. After meeting them in person, the man forced the two girls into sex work.
- In March 2019, a married couple was found guilty of conspiracy to obtain forced labor and two counts of obtaining forced labor. The couple employed foreign workers to perform domestic labor in their home in Stockton, California. The defendants used the Internet and an India-based newspaper to post false advertisements about the wages and nature of the employment at their home. Upon arrival, the workers were forced to work 18-hour days with little to no wages.
- In October 2017, a sex trafficker was convicted on 17 counts of trafficking adults and minors. Additional charges included child pornography and obstruction of justice. The perpetrator received a 33-year sentence. A victim from the Seattle area met the sex trafficker's accomplice on a dating website. The trafficker and his accomplice later promised to help the victim with her acting career. After a few months, the victim was abused and forced into prostitution.

Read the rest here:

https://www.bleepingcomputer.com/news/security/fbi-warns-of-human-traffickers-luring-victims-on-social-networks/?&web_view=true

Membership Corner

# Membership Update

Have you updated your contact information on the ISSA International website? You have! That is awesome. If you have not, please log onto the ISSA International website and click on your welcome icon on the top of the page and select “Account + Settings”. Once there you can make your updates. Thank you for your support.

| New Members April |
|---|
| Jennifer Carlson |
| Christopher J. Tarrant |
| Deidre LaCour |
| James Barrett |

I would also like to welcome our new members on behalf of the Chapter! When you’re participating in Chapter activities, please take a moment to introduce yourself to members of the board, me, and other members. Don’t forget to identify yourself as a new member and feel free to ask for help or information. Thanks for joining the Chapter and don’t forget to look for opportunities to lend your expertise to improve the Chapter. We’re always open to new ideas and suggestions.

Our membership is hanging it at ~395 members as of the end of April 2020.

Please watch the newsletter, communications and eVites to ensure you stay aware of what’s going on in the chapter. As always, if you have any membership questions don’t hesitate to contact me.

Thanks,

*Steven Mulig*

Vice President of Membership

*membership@issa-cos.org*

# NSA, ASD Release Guidance for Mitigating Web Shell Malware

By Staff, CISA, April 22, 2020

The U.S. National Security Agency (NSA) and the Australian Signals Directorate (ASD) have jointly released a Cybersecurity Information Sheet (CSI) on mitigating web shell malware. Malicious cyber actors are increasingly deploying web shell malware on victim web servers to execute arbitrary system commands. By deploying web shell malware, cyber attackers can gain persistent access to compromised networks. The CSI provides techniques to detect—and recommendations to prevent—malicious web shells.

The Cybersecurity and Infrastructure Security Agency (CISA) encourages users and administrators to review the CSI and NSA’s article, Detect & Prevent Cyber Attackers from Exploiting Web Servers via Web Shell Malware, for more information and to apply the recommended mitigations.

*(Continued from page 1)*

## A Note From Our President

our preparations for the **June online CISSP Review**. Registration for this event is open and fills up fast. Don't wait to secure your slot as seating is limited. Also launching in May is a planning committee for our **2021 30th Anniversary**! If you like to party, volunteer to help plan this event. We want this celebration to be one for the ages. It will be open to chapter members and community partners and will showcase many aspects of our chapter history. If our interested in helping out, contact our Recorder/Historian at recorder@issa-cos.org.

Before closing this letter, I want to take moment to seriously **thank** all our members and community partners who have been working hard to support those in need during the COVID-19 pandemic. Although we are beginning to see a decline in the spread of this virus, our nation will still need to remain cautious as we attempt to resume normal life. So many have selflessly spent time and personal resources to assist those in need. Such sacrifices continue to show the power of our love for others. Rest assured, our chapter is also doing all we can to help our members and our community. Not just with ongoing events but, also with our time and availability. Again, I will say, **if anyone is in need of anything, please reach out to our board of directors at info@issa-cos.org** and we will assist as best we can.

With that, I bid you all a **safe and healthy** month of May and hope to see you at one of our upcoming online events.

Sincerely,

*Ernest*

# FBI Releases Guidance on Defending Against VTC Hijacking and Zoom-bombing

Original release date: April 2, 2020

The Federal Bureau of Investigation (FBI) has released an article on defending against video-teleconferencing (VTC) hijacking (referred to as "Zoom-bombing" when attacks are to the Zoom VTC platform). Many organizations and individuals are increasingly dependent on VTC platforms, such as Zoom and Microsoft Teams, to stay connected during the Coronavirus Disease 2019 (COVID-19) pandemic. The FBI has released this guidance in response to an increase in reports of VTC hijacking.

The Cybersecurity and Infrastructure Security Agency encourages users and administrators to review the FBI article as well as the following steps to improve VTC cybersecurity:

Ensure meetings are private, either by requiring a password for entry or controlling guest access from a waiting room.

Consider security requirements when selecting vendors. For example, if end-to-end encryption is necessary, does the vendor offer it?

Ensure VTC software is up to date. See Understanding Patches and Software Updates.

CISA also recommends the following VTC cybersecurity resources:

FBI Internet Crime Complaint Center (IC3) Alert: Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments

Zoom blog on recent cybersecurity measures

Microsoft Teams security guide

# Webinars from Dark Reading!

## *They're Free!*

The following are FREE online events sponsored by Dark Reading. They are each one hour in length. Click on the link and get started.

### Preventing Credential Theft & Account Takeovers

Breaches that expose passwords and grant cyber attackers access to privileged user accounts are now so common that users greet the news with more shrugs than shock, and security experts advise to "assume user credentials have been exposed." Yet, these attacks can be as catastrophic as they are commonplace. Stolen credentials and account takeovers are the footholds cybercriminals use to launch all manner of attacks -- from financial fraud and virtual currency theft, to data breaches and cyber espionage. In this webinar learn how these bread-and-butter cyberattacks work and how to bolster your defenses against them.

http://webinar.darkreading.com/webinar/view/event/name/5863?elq_mid=95625&elq_cid=34172852&elqTrackId=484de6d4e2b048b29a07ea29030f9c6e&elq=3d3c9c8e7bd44c6e80a11f54225cd83d&elqaid=95625&elqat=1&elqCampaignId=

### 10 Incredible Ways to Hack Email & How to Stop the Bad Guys

Join us as we explore 10 ways hackers use social engineering to trick your users into revealing sensitive data or enabling malicious code to run.

http://webinar.darkreading.com/webinar/view/event/name/5631?elq_mid=92366&elq_cid=34172852&elqTrackId=9c7d66e7f40e4e76b4a6c1e64ea92cfb&elq=14e03afa5c2f4183aa75a6f66c35052f&elqaid=92366&elqat=1&elqCampaignId=

### Malicious Insiders: Real Defense for Real Business

Corporate espionage, sabotage and other security incidents could be committed or aided by any insider with something to gain from it. So how might you predict when a once-trustworthy employee is about to do something malicious? How can you give staff all the tools and access privileges they need to be productive, without leaving the organization open to unnecessary risk?

http://webinar.darkreading.com/webinar/view/event/name/5731?elq_mid=96368&elq_cid=34172852&elqTrackId=8ad577e408be4a5791490ef48328ecc1&elq=cf9ba5b65def466492f46100c9ec3639&elqaid=96368&elqat=1&elqCampaignId=

### Enterprise IoT: Rise of the Unmanaged Devices

Join IBM services and Armis, the leading enterprise IoT security company, to see real-life scenarios of these new unmanaged devices - from enterprise to healthcare to manufacturing. If you're responsible for threat management or looking how to secure unmanaged assets and IoT devices, you won't want to miss this event.

http://webinar.darkreading.com/webinar/view/event/name/5675?elq_mid=93983&elq_cid=34172852&elqTrackId=59479b654df1418186c8450235b531b8&elq=9214eddc65504c468bd9537a269b926e&elqaid=93983&elqat=1&elqCampaignId=

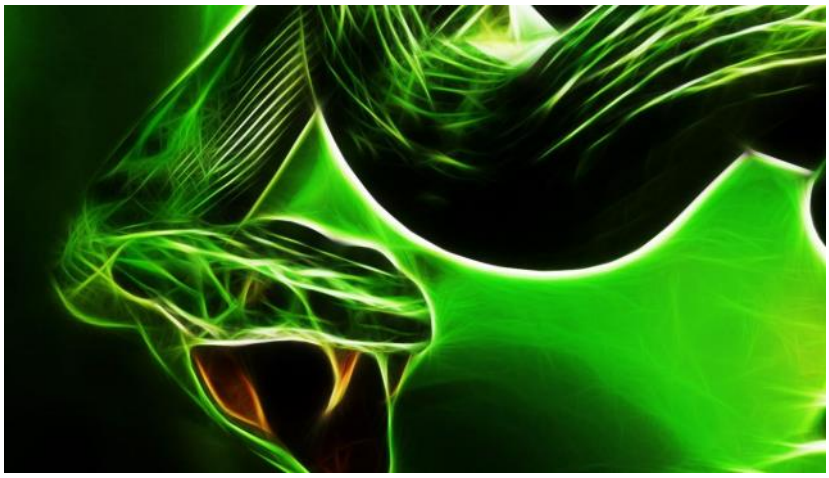
# Research shows malware is easy to buy, own, and deploy

By Jonathan Greig, TechRepublic, April 28,2020

A new study from research organization CyberNews.com found that malware is becoming increasingly easy to buy and deploy, even for those without technical backgrounds.

While malware deployments have grown in sophistication over the years, the number of attacks has also risen, signaling a democratization of tools allowing less-experienced cybercriminals to take advantage of widespread information. The report found that through underground message boards and Dark Web marketplaces, bad actors can easily find "incredibly low cost" widely available "off-the-shelf malware and ransomware."

"What we found exceeded our expectations far beyond what we initially anticipated. As it turns out, you don't have to be a programmer or even have any specialized technical knowledge to buy or create malware. In fact, the entry bar is set so low that practically anyone can do it–all you need is an online wallet loaded with some Bitcoin," the report said.



"Encrypted trojans that can remain undetected by even the most sophisticated antivirus systems? Custom-built ransomware tailored to your own specifications? Remote cybercrime courses for aspiring 'online entrepreneurs?' It's all there and available for would-be cybercriminals–for the right price."

CyberNews researchers looked at 10 so-called DarkNet marketplaces and found that buying malware is easy and fast, with cheap or even free programs allowing people to own malware. For just $50, would-be criminals can buy advanced tools on cybercrime forums that operate in the open, it found.

According to its investigation, there is even customer support for malware tools that you can buy that include free updates as well as troubleshooting services.

"In the many shadow markets of today, malware is easily bought, sold and traded on websites that are basically Dark Web versions of Craigslist. Some malware marketplaces are easy to find and open to anyone. Most of the malware tools sold in these entry-level websites are of inferior quality, made by neophyte hackers looking to make their names in cyberspace," the report said.

"On the other end of the spectrum are invite-only message boards, accessible only via the TOR network and run by veteran Eastern European cybercriminals who offer high-grade products used by serious clientele."

The key to using malware is not skill but simply knowing how to find malware tools and there are a number of websites that provide detailed lists of forums where these tools are available. CyberNews researchers noted that one website has organized a list of places people can buy and sell malware that is organized by country.

In an email interview, CyberNews PR manager Lina Bernotaityte explained that its difficult to pinpoint who exactly is behind these malware tools and all the features accompanying them, but even with their anonymity, it is safe to say that these malware creators come from countries and regions where cybercrime legislation is not strictly enforced and talented, tech-inclined people don't have many opportunities for gainful employment.

The report notes that a number of malware creators offer their tools for free to a select group of cybercriminals as a way to make sure they work and increase usage as well as future potential for payment.

CyberNews researchers wrote that they were able to find a wide variety of malware brands for sale with everything from banking trojans to ransomware builders and "modular malware bots."

Read the rest here:

https://www.techrepublic.com/article/research-shows-malware-is-easy-to-buy-own-and-deploy/

# Dispelling Zoom Bugbears: What You Need to Know About the Latest Zoom Vulnerabilities

By Tod Beardsley, Rapid7, April 2, 2020

A recent lawsuit filed regarding the infamous 2017 Equifax data breach revealed that the company was using "admin" as a username and password to protect sensitive data from 147 million customers — even though this password has been exposed through data breaches almost 50,000 times, according to the Have I Been Pwned database.

Wow, this past week has been a pretty long year for Zoom.

As the COVID-19 global pandemic moved the whole knowledge-working world abruptly to work-from-home, virtual meetings are rapidly becoming *de rigueur* for pretty much everyone I know. As a result, Zoom's stock price hit an all-time high in mid-March (despite the stock market being depressed overall), trading on massive volume and suddenly seeing a PE ratio well north of 1500x. Thanks to its insanely easy-to-use cross-platform video conferencing service, Zoom was a successful B2B company well before the pandemic. Today, it's a household name beyond airport billboards as apparently everyone has been transformed into consumers and fans while we're all steering clear of other humans.

Well, almost everyone. Turns out, all this recent success has painted a huge target on Zoom's back, and people are falling all over themselves every time a new security issue is discovered in the platform, no matter how minor. Because of this, I wanted to take a little bit of your time—and mine—to discuss the Zoom-related scuttlebutt that has surfaced over the past few days. But, if you don't have time to get into it, the TL;DR summary is best summed up as:

> *Yes, Zoom has some security issues. It's complex software. All complex software has bugs. Some of those bugs are security-relevant. The engineers, marketers, and leadership at Zoom are neither dumb nor evil. You can judge Zoom on its response to security issues, more so than on the security issues themselves, within reason.*

Before we jump into the issues, a bit of full disclosure: Rapid7 is a happy Zoom customer, and has been for a while now. Personally, I kind of love the software and service, and prefer it over every other video conferencing solution I've had my hands on, pretty much ever. I'm hopeful this doesn't make me a craven apologist, but do let me know if I haven't been able to adequately manage my own biases.

Okay. Here we go, in as close to chronological order of mainstream reporting as I can manage:

## Zoom leaking data to Facebook

**The gossip:** Zoom leaks personal information to Facebook, even if you're not a Facebook user.

**The reporting:** Joe Cox, writing for Vice Motherboard, reported on March 26, 2020, that Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account. The article accurately illustrates what went down with Zoom's usage of the Facebook software development kit (SDK) on Apple platforms that run iOS (namely, iPhones and iPads), and it appears that Joe is the original researcher who first reported the issue to Zoom.

**What's happened since:** Zoom has pulled the Facebook SDK from its iOS app for Apple platforms by removing the "Login with Facebook" feature.

The updated Motherboard article does indeed confirm that Zoom acted within days by removing the leaky feature. (Zoom's blog post claims it was under two days, but who's counting?) It does not appear that Zoom was transmitting this information on purpose (let alone, selling it), and the personal information being leaked was basic diagnostics about the phones and tablets—things like screen size and storage space, along with some coarse location data. Importantly, it wasn't things like usernames, passwords, phone numbers, or nuggets of information from conversations. Motherboard also reports that Facebook was, in turn, setting a cookie-like unique ID for users, presumably for advertising.

Read the rest here:

https://blog.rapid7.com/2020/04/02/dispelling-zoom-bugbears-what-you-need-to-know-about-the-latest-zoom-vulnerabilities/

# ISSA Fellow Program

## 2020 Fellows Cycle Now Open

The Colorado Springs ISSA Chapter has over 400 current members. Many of you have been members for several years and may qualify for the ISSA fellow program. The Fellow Program recognizes sustained membership and contributions to the profession. If you think you or another ISSA associate may qualify in the Fellow Program, once the 2020 award criteria is made available please contact Colleen Murphy at past-president@issa-cos.org to help you through the steps. Below are some details on the ISSA Fellow Program. Qualification information is also presented below:

No more than 1% of members may hold Distinguished Fellow status at any given time. Fellow status will be limited to a maximum of 2% of the membership.

Nominations and applications are accepted on an annual cycle. Applications will be accepted in the near future, and details will be provided in a future newsletter. Following the application period, there will be a ten week review period followed by the notification and presentation process. Fellows and Distinguished Fellows will be recognized at the 2020 ISSA International Conference.

## *To Become a Senior Member*

Any member can achieve Senior Member status. This is the first step in the Fellow Program. What are the criteria?

**Senior Member Qualifications**

- 5 years of ISSA membership
- 10 years relevant professional experience
- For your convenience, we will have available the Senior Member Application Check-list to confirm eligibility and completion of application

All Senior Member applications require an endorsement from their home chapter to qualify.

## *To Become a Fellow or Distinguished Fellow*

Have you led an information security team or project for five or more years? Do you have at least eight years of ISSA membership and served for three years in a leadership role (as a chapter officer or Board member or in an International role)? You may be eligible to become an ISSA Fellow or Distinguished Fellow.

**Fellow Qualifications**

- 8 years of association membership.
- 3 years of volunteer leadership in the association.
- 5 years of significant performance in the profession such as substantial job responsibilities in leading a team or project, performing research with some measure of success or faculty developing and teaching courses.

All Fellow applications require a nomination to qualify.

**Distinguished Fellow Qualifications**

- 12 years association membership.
- 5 years of sustained volunteer leadership in the association.
- 10 years of documented exceptional service to the security community and a significant contribution to security posture or capability.

All Distinguished Fellow applications require a nomination to qualify.

*https://458rl1jp.r.us-east-1.awstrack.me/L0/https:%2F%2Fwww.issa.org%2Ffellows-program%2F/1/01000171dcdf328e-1f321b60-127b-44e5-a53d-39fa514c70c5-000000/_QtQ0l9nkskTqK4YDlJgaD08HQQ=160*

# 2020 ISSA Awards Program

We are continually monitoring and making the best decisions we can, based on the health and welfare of our members, our staff, and our community at large. Given the nature and uncertainties surrounding this pandemic, we have decided to move our annual awards ceremony and dinner to a new date in the fall. The new date and details will be published as soon as we have confirmed our plans.

**In this spirit we have decided to extend the ISSA Awards and ISSA Fellows Program nomination and entry deadline to July 25, 2020.**

**NOMINATE NOW!**

As cyber security professionals your voices and opinions are the most valuable when it comes to providing awareness of peers and organizations in our communities doing incredible work to propel our industry forward. *They deserve to be noticed* so please honor them with a nomination to one of the following awards:

- Hall of fame
- Honor Role
- Chapter of the Year
- Volunteer of the Year
- Organization of the Year
- Presidents Award for Public Service
- Security Professional of the Year

For details on each category and to nominate **click here**

The ISSA Fellows Program honors established cyber professionals with demonstrated success and contributions to the industry. These individuals have dedicated years towards the innovation and progression within the cyber realm.

For more details and to nominate a notable individual please **click here:**

We appreciate your participation and time in helping to recognize our shining stars in the community.

Thank you.
*Marc Thompson*
Executive Director
ISSA International


# How to secure sensitive data and technology when a remote employee leaves

By Macy Bayern, TechRepublic, April 27, 2020

No less than 98 per cent of traffic sent by internet-of-things (IoT) devices is unencrypted, exposing huge quantities of personal and confidential data to potential attackers, fresh analysis has revealed.

With COVID-19 shaking up employment, many teams are facing furloughs and layoffs. Some employees, however, are also opting to leave their jobs during this chaotic time. No matter the reason, companies must have the proper plans and security in place for an employee's departure.

Companies have been forced to quickly adapt to remote work because of the coronavirus, many of which have never worked entirely remotely previously.

"Organizations are frantically trying to enable existing workforces to become full-time remote workforces," said Arun Kothanath, chief security strategist at Clango, an identity and access management (IAM) consultancy. "This requires organizations to rapidly roll out VPNs and authentication technologies, such as multi-factor authentication, while enabling employees to be able to connect to mission-critical assets from their remote workstations."

While equipping employees with secure connections is one of the crucial first steps to launching a remote workforce, businesses must also consider how to rescind such access upon employee termination or departure.

"The only way to secure critical business data is to control the access to it," Kothanath said. "When an employee is terminated or informs the organization they are leaving for another company, there must be a way for an IT manager to immediately revoke the employee's access."

Neal Taparia, co-founder of SOTA Partners, said he once experienced an employee send themselves sensitive business information upon figuring out their employment would be terminated.

To help prevent other organizations from facing similar situations, Taparia and other experts outlined the following best practices for keeping company information and hardware secure in the event of an employee leaving.

## IT's responsibility for when an employee departs the company

- **Remove email access**

After Taparia's bad experience, he said the first thing his company does is shut off access to the employee's email, that way the employee can't send themselves items.

"We'll also quickly peruse the type of activity they've had in their Google accounts. We use the Google Apps Productivity Suite, and it gives you some administrative abilities to see what's going on," Taparia said.

"We'll look for any type of suspicious behavior, and we'll try not to signal to [employee] that we're going to have this tough conversation so they have time to [transmit sensitive files]," he added.

- Confiscate company hardware

One problem employers might run into is how to retrieve company hardware from its remote workers.

Taparia said companies should make this process easy. His organization provides a box with a shipping label for the worker to send their items. He also said to guarantee the employee sends hardware back, his organization leverages severance.

"We try to get them a box with a shipping label as fast as possible, and we'll tell them, 'We want to give you the severance, but we do need that equipment back as soon as possible. If you want full severance, we need that back ASAP, and we're going to make it as easy for you as it is possible to put it in the box and put the shipping label on it and just get it back to us,'" Taparia said.

- **Return in-office items**

Read the rest here:

https://www.techrepublic.com/article/how-to-secure-sensitive-data-and-technology-when-a-remote-employee-leaves/

# The Pentagon's Cybersecurity Certification Plan Includes Continuously Monitoring Contractors

By Mariam Baksh, Nextgov, April 22, 2020

The accreditation body overseeing the Defense Department's Cybersecurity Maturity Model Certification program—the CMMC-AB—issued a request for proposal that provides insight into how the group plans to keep track of contractors outside of conducting physical audits.

The CMMC will end the DOD's practice of allowing contractors to "self-certify" their cybersecurity practices. Before the end of the year, the department intends to require companies doing business with the DOD to gain a certificate from third-party auditors that will be valid for up to three years.

"As part of the CMMC-AB's efforts to mitigate risks posed to the country through sharing of sensitive information with DOD supply chain partners, a continuous monitoring solution will help fill in the gaps between assessments scheduled for once every three years," the RFP reads. "The CMMC-AB is issuing this request for proposal to help us identify appropriate partners in our continuous monitoring solution."


The CMMC-AB posted the RFP to its LinkedIn page earlier today with a May 1 deadline for responses.

Katie Arrington, chief information security officer for the Defense acquisition office, who has embraced the alternative title "mother of the CMMC," mentioned the RFP during a webinar today on the DOD's efforts to help small businesses amid the coronavirus pandemic.

She was responding to a question about how the coronavirus would affect the timeline for implementing the CMMC.

Arrington has previously said the program would be unaffected, noting that the training for assessors would largely take place online anyway.

But last week during a Bloomberg Government webinar she conceded the virus is "affecting every aspect of our lives" and that there may be a delay in initial audits by about two weeks.

Today, she seemed to give herself more flexibility but pointed to other areas, such as the CMMC-AB's RFP, where the program is still moving full speed ahead.

"The training and the audits are based with a portion in person, and until we get the directive from the president and [Defense] Secretary Esper, we have our stay at home orders and [are] only mission-critical and trying to keep our meetings in-person to a minimal, so stay tuned, we're still doing our absolute best to stay on track."

Arrington said the plan is still to roll out the first class of auditors in late May, early June. The audits have to happen in-person, on-site, she stressed but noted the DOD is working with the "pathfinders" who will undergo the initial reviews.

## Inside the Portal

The chief requirements for respondents to the RFP is that the partner entity "accept and secure AB and DOD Intellectual property" and create a secure portal that would allow various stakeholders access to varying degrees.

According to the RFP, organizations seeking certification, assessors and certified third-party assessment organizations known as C3PAOs "will all utilize the CMMC-AB's continuous monitoring solution to conduct pre-assessment background research as well as monitor companies between formal assessments."

Defense officials have stressed their independence from the CMMC-AB. While the portal should support multi-factor access with the department's Common Access Card, authorized DOD staff would only have "read only" access. They should, however, be able to "search for and view information on any company in the database and to access aggregated metrics from across all monitored companies and defined subsets thereof," the RFP states.

Assessors and their C3PAOs, meanwhile, should be able to receive automatic notifications when any company they were responsible for assessing has a security score decrease a specific, to be determined amount, according to the RFP.

Read the rest here:

https://www.nextgov.com/cybersecurity/2020/04/pentagons-cybersecurity-certification-plan-includes-continuously-monitoring-contractors/164821/

# 2020 Schedule of Events

***Chapter Meetings – Dinner (5:30 – 7:30 PM)***
Tuesday, July 21, 2020
Tuesday, August 18, 2020
Tuesday, October 20, 2020
Tuesday, November 17, 2020

***Mini-Seminars – Breakfast (8:30 – 12:00 PM)***
Saturday, July 25, 2020
Saturday, August 22, 2020
Saturday, October 24, 2020
Saturday, November 14, 2020

***Security + CE Reviews***
Saturday, September 12, 2020
Saturday, September 19, 2020
Saturday, September 26, 2020

***ISSA-COS Conferences***
***Peak Cyber (PC) Symposium***
Tuesday, September 15, 2020
Wednesday, September 16, 2020
Thursday, September 17, 2020

***CISSP Review***
Friday, June 5, 2020
Saturday, June 6, 2020
Saturday, June 13, 2020
Friday, June 19, 2020
Saturday, June 20, 2020
Saturday, June 27, 2020
Member Fee: ~~$200~~ ** Now **$100** **
Non-member Fee: ~~$600~~ ** Now **$300** **

***Chapter Meetings – Lunch (11:00 – 1:00 PM)***
Wednesday, July 22, 2020
Wednesday, August 19, 2020
Wednesday, October 21, 2020
Wednesday, November 18, 2020

For additional information, contact info@issa-cos.org or visit www.issa-cos.org.

---

**05/14/2020 / Session 2**

**Speaker #1: Mr. Trent Brunnell,** *ISSO, LinQuest*

**Topic: How the Risk Management Framework is utilized to keep government systems secure**

**Speaker #2: Mr. Peter Sopczak,** *ISSM, Pluribus*

**Topic: Incident Response**

**05/21/2020 / Session 3** **Paid Sponsor:** semperis

**Speakers: Mr. Sean Deuby,** *Director of Services, Semperis* **| Mr. Clark Brown,** *Partner and Practice Leader, Alescent*

**Topic: Ransomware vs. Active Directory Backups: What Can Throw a Wrench into Your Disaster Recovery Process?**

**05/28/2020 / Session 4**

**Speaker: Ms. Erin Plemons,** *Cybersecurity Engineer, ENSCO*

**Topic: Practical Cyber Assessments for Automation Systems** *(ft. Ms. Lori Hayes)*

# SPECIAL INTEREST GROUPS (SIGS)

## SIG Overview

The ISSA-COS Special Interest Groups (SIGs) are comprised of Cybersecurity professionals who gather to share information and experiences common to their respective groups. ISSA-COS presents SIGs in two major categories: **Affinity Groups** and **Industry Groups**. Through our online forum, ISSA-COS enables our members and the community at large to participant in thoughtfully organized and well-structured categories of conversation. Forum participants can engage in any one of eight different SIGs. Within our forum, we commission Subject Matter Experts who add increased technical knowledge to all the conversational threads.

To maintain positive behaviors within the forum, ISSA-COS has assigned a SIG Program Coordinator who monitors each SIG conversation. The SIG Program Coordinator also monitors the size and degree of participation within each SIG. Once participation reaches a sizable amount, the SIG Program Coordinator will suggest and help organize in-person meet ups. This provides SIG participants an opportunity to put virtual names with physical faces to further strengthen the bonds of interaction taking place in the virtual environment.

## Affinity Groups

Affinity Groups are designed for community professionals with like-minded interests in the field of Cybersecurity. Affinity Groups share security related experiences, impart knowledge and education, and help one another solve common problems and issues. The Affinity Groups currently promoted by ISSA-COS include:

- Women in Security (WIS)
- Young Professional in Security (YIS)
- Educators in Security (EduIS)
- Executives in Security (ExecIS)

## Industry Groups

Industry Groups are designed for community professionals who work within similar industries and have a common interest in Cybersecurity. Industry Groups discuss security related topics and share solutions to problems affecting their perspective industries. They also exchange Cybersecurity related tips, information, and education specific to their industries. The Industry Groups currently promoted by ISSA-COS include:

- Finance in Security (FIS)
- Healthcare in Security (HIS)
- Retail in Security (RIS)
- DoD in Security (DodIS)

# Peak Cyber Symposium – *10th Anniversary!*

The Peak Cyber Symposium is an annual 3-day event that attracts over 500 attendees from across the nation. This event kicks off with a full day of Capture-the-Flag (CTF) fun and competition. A morning CTF prep session for beginners followed by the actual competition in the afternoon. Lunch is provided and snacks are served throughout the day.

**Sept. 15-17, 2020**
**DoubleTree Hotel**
**Register at:**
**www.issa-cos.org**
**info@issa-cos.org**

The following 2-days include a series of keynote speakers, panel discussions, breakout sessions, and an exhibitor hall. Community representatives from partnering organizations are on hand to educate and inform attendees on events coming up within the community. Each annual Peak Cyber Symposium emphasizes an industry relevant theme.

*Highlights for this event include:*

- Nationally recognized Keynote Speakers and Fortune 500 Sponsors/Exhibitors
- Up to 24 potential Continuing Professional Educations (CPE) Credits Available
- Over 100 Capture-the-Flag participants - all skill levels are welcome – *beginners too!*
- Over $10,000 in prizes and giveaways
- Networking, Networking, Networking!!
- 40 Exhibitor Booths with Live Demos
- Free parking, Free breakfast, Free afternoon snacks.

# *Update Your Profile!*

Don't forget to periodically logon to *www.issa.org* and update your personal information.

# 2020 Peak Cyber Symposium Sponsors

MURRAY SECURITY SERVICES — Platinum

Hewlett Packard Enterprise — Silver

splunk> — Bronze

EPOCH CONCEPTS AGILE MINDS. POWERFUL CHANGE. — Bronze

## Exhibitors

MURRAY SECURITY SERVICES | Hewlett Packard Enterprise | Jacobs | splunk> | EPOCH CONCEPTS AGILE MINDS. POWERFUL CHANGE.

**Become a 2020 Sponsor Today!**
**For more information email: sponsorships@issa-cos.org**

# Strategic Partnership - IAPP

## Membership Benefits

- Savings on **worldwide events to inform** you of new developments and promote professional connections
- **Critical industry perspective** delivered free to your inbox daily, weekly or monthly with IAPP's insightful reporting
- Free access to collections of privacy-related **literature, research and tools**
- **Savings on training** programs to magnify your industry expertise
- Earn the industry's most **trusted certifications** and designations
- **Global networking** opportunities with colleagues putting privacy on the map

# MENTORING PROGRAM

The ISSA-COS Mentoring Program provides a connection between individuals (mentees) seeking career guidance, industry information, or personal encouragement with individuals (mentors) who have an aptitude for sharing their career experiences, industry resources, and personal talents for the benefit of the mentee. Mentees derive from every conceivable background and exist at every stage of professional development. Mentoring sessions are designed to ensure the confidentiality, integrity, and availability of information shared between the participants.

To help facilitate the mentoring process, ISSA-COS has adopted the S.M.A.R.T. goal setting model to safeguard a consistent development process that is equally understood and honored by mentees and mentors alike. As such, the Mentoring Program supports the following objectives of ISSA-COS:

**For more information about mentoring, email: *mentorship@issa-cos.org***

- Promote increased professional education opportunities for members
- Provide career guidance and professional development approaches
- Encourage balance between technical skillsets and soft skills such as time management, task management, workplace conduct, and business savvy
- Increase member knowledge of available resources designed to strengthen skillsets
- Encouraging an open exchange of Cybersecurity related techniques, approaches, and problem-solving skills
- Promote member education and awareness of Cybersecurity security issues and recommended strategies to combat the issues
- Providing opportunities for mentees and mentors to network with other professionals and share their lessons learned from their individual mentoring experiences.

# 2020 Chapter Sponsors

Platinum (ACS, CFS, PCS)

Bronze (ACS, CFS, PCS)

Bronze (CFS, PCS)

Bronze (CFS, PCS)

Venue Sponsors

# Become a Sponsor!

- **Annual Chapter Sponsor (ACS)**
- **Cyber Focus Symposium (CFS)**
- **Peak Cyber Symposium (PCS)**
- **Financial Sponsors**
- **Conference Exhibitors**
- **Material Sponsors**
- **Single Event Sponsors**

For more information about sponsorship opportunities, email:

**sponsorships@issa-cos.org**

Jacobs

ISSA
Information Systems Security Association
Colorado Springs Chapter
www.issa-cos.org

ISSA-COS WELCOMES **JACOBS** AS OUR NEWEST ANNUAL CHAPTER SPONSOR!

**THANK YOU, JACOBS** FOR SUPPORTING OUR CHAPTER, OUR MEMBERS, AND OUR COMMUNITY!

**BRONZE**

ANNUAL CHAPTER SPONSOR

Hewlett Packard Enterprise

ISSA
Information Systems Security Association
Colorado Springs Chapter
www.issa-cos.org

ISSA-COS WELCOMES **HP ENTERPRISE** AS OUR NEWEST CONFERENCE SPONSOR!

**THANK YOU, HPE** FOR SUPPORTING OUR CHAPTER, OUR MEMBERS, AND OUR COMMUNITY!

**BRONZE**

2020 PEAK CYBER SYMPOSIUM SPONSOR

# Strategic Partnership – Discover Goodwill

Discover Goodwill
Southern & Western Colorado


Free Security + training and exam for qualified applicants.
Contact **info@issa-cos.org** or more information or to apply.

splunk>

EPOCH CONCEPTS
AGILE MINDS. POWERFUL CHANGE.

ISSA
Information Systems Security Association
Colorado Springs Chapter
www.issa-cos.org

ISSA-COS WELCOMES **SPLUNK AND EPOCH CONCEPTS** AS OUR NEWEST CONFERENCE SPONSOR!

**THANK YOU** FOR SUPPORTING OUR CHAPTER, OUR MEMBERS, AND OUR COMMUNITY!

**BRONZE**

2020 PEAK CYBER SYMPOSIUM SPONSOR

# Join ISSA-COS on Social Media

Twitter:
- Colorado Springs ISSA
- @COSISSA

LinkedIn:
- ISSA Colorado Springs Chapter
- https://www.linkedin.com/groups/1878203/

Facebook:
- Colorado Springs Chapter of the ISSA
- @ColoradoSpringsISSA

# Strategic Partnership – NCX

## Available Resources

- **ISSA-COS Agreement: CyberAlliance+**
- **Membership Plans**
- **Technical Forums**
- **LegalShield**
- **IDShield**
- **Pre-recorded Webinars**

# ISSA-COS Community Partners


## ISSA Nametags

Do you want an ISSA nametag for your very own to wear to meetings, conferences, and events? You can now order/pick up yours directly from:

*Blue Ribbon Trophies & Awards*
*245 E Taylor St (behind Johnny's Navajo Hogan on North Nevada)*
*Colorado Springs*
*(719) 260-9911*

Although their hours are officially Monday through Friday until 5:30 pm, they are occasionally in the shop on Saturdays. This is a small business so cash/check would be appreciated. Email wbusovsky@aol.com to order.

# 2020 Annual Chapter Sponsorship Plans

## For more information email: sponsorships@issa-cos.org

| ISSA-COS Annual Financial Sponsorship Packages | Platinum | Gold | Silver | Bronze | Single Event |
|---|---|---|---|---|---|
| | $19,995 | $14,995 | $9,995 | $4,995 | $2,495 |
| **Name/Logo recognition in the following channels** | | | | | |
| a. Chapter website | X | X | X | X | X |
| b. Mass-marketing emails | X | X | X | X | X |
| c. Monthly newsletter | X | X | X | X | X |
| d. On-screen recognition at scheduled events | X | X | X | X | X |
| **Preferred Guest Speaker for the following events** | | | | | |
| a. Cybersecurity Special Events | X | X | X | X | X |
| b. Chapter Meetings and Mini Seminars | X | X | X | | |
| c. Cyber Focus Symposium | X | X | | | |
| d. Peak Cyber Symposium | X | | | | |
| **Discounted Exhibitor Packages for conferences** | | | | | |
| a. Cyber Focus Symposium: 5' x 8' (Full Price: $1,495) | -$500 | -$400 | -$300 | -$200 | -$100 |
| b. Peak Cyber Symposium: 5' x 8' (Full Price: $1,495) | -$500 | -$400 | -$300 | -$200 | -$100 |

| Material Sponsors | | |
|---|---|---|
| Type | Qty | Fee |
| Training Vouchers | 12 | $12,000 |
| Shirts | 250 | $4,000 |
| Padfolios | 250 | $2,200 |
| Lapel Pins | 250 | $800 |
| Book Bags | 250 | $400 |
| Notepads | 250 | $200 |
| Pens | 250 | $150 |
| Stickers | 250 | $100 |
| Logo Socks | 250 | $2,500 |
| Logo Beanies | 250 | $3,000 |
| Sponsor's Choice | 250 | TBD |
| Venue/Facility | n/a | $0 |

# Cyber Spotlight – PARTY!!

# ISSA-COS is turning 30 in 2021!

## Initiative to document ISSA-COS Chapter History

Interviews with past/current **Presidents**

Interviews with past/current **Board Members**

Interviews with past/current **General Members**

Interviews with **Community Partners**

ISSA Information Systems Security Association
Colorado Springs Chapter

WWW.ISSA-COS.ORG

**The Information Systems Security Association (ISSA) ® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.**

**The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity, and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved. Members include practitioners at all levels of the security field in a broad range of industries such as communications, education, healthcare, manufacturing, financial, and government.**

***Chapter Officers:***

President*: Ernest Campos
Vice President*: Michael Crandall
Executive Vice President*: Scott Frisch
Treasurer: Dennis Schorn
- Deputy: **Vacant**

Recorder/Historian: Andrea Heinz
- Deputy: **Vacant**

Dir. of Professional Outreach: Katie Martin
- Deputy: **Vacant**

Director of Communications : Christine Mack
- Deputy: Ryan Evan

Director of Certifications: Derick Lopez
- Deputy: Luke Walcher

Vice President of Membership: Steven Mulig
- Deputy: **Vacant**

Vice President of Training: Mark Heinrich
- Deputy: Phebe Swope

Member at Large: Art Cooper
Member at Large: Jim Blake
Member at Large: James Asimah
Member at Large: Dennis Kater

***Committee Chairs:***

Training: Mark Heinrich
Mentorship Committee Chair: **Vacant**
Media/Newsletter: Don Creamer
IT Committee: Patrick Sheehan
Speaker's Bureau: William (Jay) Carson

**** Executive Board Members***

## Article for the Newsletter?

We are always looking for articles that may be of interest to the broader Colorado Springs cyber community.

Send your article ideas to the Newsletter at:

*newsletter@issa-cos.org*

## *Past Senior Leadership*

President Emeritus: Dr. George J. Proeller
President Emeritus: Mark Spencer
Past President: Pat Laverty
Past President: Cindy Thornburg
Past President: Frank Gearhart
Past President: Colleen Murphy

## Academics turn PC power units into speakers to leak secrets from air-gapped systems

By Catalin Cimpanu, ZDNet, May 4, 2020

Academics from an Israeli university have published new research last week showing how an attacker could turn a computer's power supply unit into a rudimentary speaker that can secretly transmit data from an infected host using audio waves.

The technique, named POWER-SUPPLaY, is the work of Mordechai Guri, the head of R&D at the Ben-Gurion University of the Negev, in Israel.

Read the rest here:

https://www.zdnet.com/article/academics-turn-pc-power-unit-into-a-speaker-to-leak-secrets-from-air-gapped-systems/

***Published at no cost to ISSA Colorado Springs by Sumerduck Publishing TM, Woodland Park, Colorado***