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

Colorado Springs, Colorado

ISSA-COS NEWSLETTER

VOLUME 9 NUMBER 4 APRIL 2020

Tough Times

A Note From Our President

By Mr. Ernest Campos

Fellow Members of ISSA-COS,

What an unprecedented time we find ourselves living in. COVID-19 has made quite an impact on society; both professionally and personally. As I write this letter, our chapter has had to cancel all in-person events from as far back as mid-March and likely, we may not be able to resume normal activities until July. We now find ourselves deep enough into this global pandemic that most of us here in Colorado Springs have been personally affected by the virus; either directly or indirectly through someone we know or love. The emotional impact is also setting in as we are forced to decrease human interactions and take shelter at home; both for work and for our families.

And yet, through it all, we see the power of human kindness, love, service, and sacrifice rising all around us. Healthcare workers and manufactures, first responders, and other essential services are stepping beyond any normal level of expectancy required of them. Restaurants faced with possible closures due to the lack of customers are embracing the opportunity to help those in need. Together, they are pooling their resources to provide free meals, by the dozen and by the hundreds, each day to essential personnel. I even know of single mothers who are preparing and delivering homemade meals to area school kids who normally qualify for free/reduced meals at school but are now missing out because they are forced to say at home. And on the technical front, IT companies and professionals are giving their own time and expertise to enable schools, churches, and other non-technical institutions the ability to continue operations via online conferencing tools. Indeed, people are powerful.

Recently, I participated in an online meeting with area leaders from other organizations who represent our community partners. I was impressed at the efforts underway by so many others. And, I was proud that our chapter was able to report our own efforts to help keep Cybersecurity professionals connected, engaged, and learning during these uncertain times. Our efforts may not rival the heroic activities of healthcare workers and first responders but, for what we do, our efforts are important and significant in their own way.

In under 10 days, our volunteers from within our chapter helped put together a

(Continued on page 4)

Your Social Security Number Costs $4 On The Dark Web, New Report Finds

By Jesse Damiani, Forbes, March 25, 2020

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

A new investigation conducted by Atlas VPN based on Flashpoint Intelligence research findings between 2017 and 2019 has uncovered the approximate cost of popular goods and services on the dark web.

Social Security Numbers, despite being widely regarded as outdated and insecure, particularly in the wake of the 2018 Equifax hack, are still used as the primary means of identity verification. As with Equifax, cyberattacks are often targeted at sites that will yield millions of SSNs at a time, allowing cybercriminals to steal "in bulk."

"These steps are especially important amid an increase in cybersecurity threats as a result of the COVID-19 pandemic."

Which helps explain the revelation that any individual SSN can retail for as little as $4 on the darknet.

And for that low cost, buyers often receive more than just somebody's Social Security Number. According to Flashpoint, services sold on the dark web can be divided into four primary categories:

1. PII (personally identifiable information)
2. Stolen financial information
3. Forged documents
4. Hacker services

For $4, in addition to the SSN, PII packages typically include the victim's full name, driver's license number, passport number, and email address.

Financial information tends to be slightly more expensive than PII. Atlas VPN found that access to:

- Compromised bank accounts with a $10,000 balance cost $25.
- Credit cards with $1k-5k balance cost $10.

Notably here: a victim's credit score also impacts the price, with better scores going for higher price tags. A good credit score makes it easier for cybercriminals to commit fraud without financial institutions cutting them off.

Interestingly, the price also depends on the victim's credit score. The better the score, the higher the rate. Financial institutions view a good credit score favorably, which makes it easier to commit fraudulent transactions.

Forged documents command the highest asking prices, with physical passport prices ranging from $2,980 to $5k. Meanwhile, the report found that a one-hour Distributed Denial-of-Service (DDoS) attack, in which targeted servers are overwhelmed and effectively shut down, cost approx. $165. That cost increases by 2-5x when it involves attacking a government or bank website.

While these types of hacks and sales are ultimately impossible to prevent, individuals can take critical steps to safeguard accounts and information. Obviously, be as careful as is humanly possible with SSNs and passwords, and try to select security questions that involve answers that aren't easily discoverable on the web.

But two of the best steps you can take to secure your accounts that are often overlooked are freezing credit lines and securing your mobile devices.

Credit accounts can be frozen for free at the three major reporting bureaus (Equifax, Experian, and TransUnion). This restricts access to your records so new credit files cannot be opened in your name until your account has been unfrozen.

Mobile devices, meanwhile, are notorious sites of scamming. There are simple techniques that will make you more difficult to hack, and to make it easier for you to identify if you've become the victim of identity theft.

- Be sure to have a password on your phone and consider using a PIN to access your account.
- Be vigilant with Bluetooth, public Wi-Fi, and downloading free apps—all of which can be used to gain access to your device.
- Enable two-factor authentication (2FA) whenever possible, with preference toward 2FA apps, such as Authy and Google Authenticator rather than SMS texts.

Read the rest here:

https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?&web_view=true#427b929b13f1

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 March
Seth Foley
Michael Fragola
Carl Landers
Timothy Chessmore
Tracy Vandeventer
Jeri M. La May
Lewis Johnson
Peter Rivera
Tani Evans

Join me in welcoming 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 ~400 members as of the end of February.

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

Internet Archive offers 1.4 million copyrighted books for free online

By Timothy B. Lee, Ars Technica, March 28, 2020

One of the casualties of coronavirus-related social distancing measures has been public libraries, which are shut down in many communities around the world. This week, the Internet Archive, an online library best known for running the Internet's Wayback Machine, announced a new initiative to expand access to digital books during the pandemic.

For almost a decade, an Internet Archive program called the Open Library has offered people the ability to "check out" digital scans of physical books held in storage by the Internet Archive. Readers can view a scanned book in a browser or download it to an e-reader. Users can only check out a limited number of books at once and are required to "return" them after a limited period of time.

Until this week, the Open Library only allowed people to "check out" as many copies as the library owned. If you wanted to read a book but all copies were already checked out by other patrons, you had to join a waiting list for that book—just like you would at a physical library.

Of course, such restrictions are artificial when you're distributing digital files. Earlier this week, with libraries closing around the world, the Internet Archive announced a major change: it is temporarily getting rid of these waiting lists.

Read the rest here:

https://arstechnica.com/tech-policy/2020/03/internet-archive-offers-thousands-of-copyrighted-books-for-free-online/

(Continued from page 1)

A Note From Our President

weekly series of online presentations. Not necessarily a huge feat but, one never before attempted in the history of our chapter. On Thursday, April 2, 2020 ISSA-COS hosted our first ever online presentation. Despite having only 5 days to promote the event, over 60 people registered to participate. And with only a few minor "opportunities for future improvement," it was an overall success. I applaud the efforts of our IT Committee, Speakers Bureau Committee, and our Director of Communications for making these presentations a new possibility for our chapter. Great job team!

As I close this letter, I'll turn attention toward the future beyond the current pandemic. Later this year, we look forward to the 10th Anniversary of our annual Peak Cyber Symposium (PCS). This year, PCS will take place Sep. 15-17 at the DoubleTree Hotel. We have already secured a number of great sponsors and exhibitors. Plus, this year we are doubling the size of our exhibitor space by moving it from the hallway to an actual hall. Look for guest speaker, sponsor, and early bird registration to all open soon.

Last of all, 2021 will mark our chapter's 30th birthday. Efforts are already underway to develop a full history of our chapter. This will include interview with board members, general members, and community partners. We are also planning a grand celebration to mark the occasion. More information will soon follow.

In closing, I hope and pray all our members remain safe and relatively unaffected by the COVID-19 virus. Perhaps a bit inconvenienced but, safe none the less. Many of our board members have ask me to share with you their willingness to help with any needs that may arise. If you need help, please reach out to our board at info@issa-cos.org and we will do all we can to assist you.

Sincerely,

Ernest

March 23, 2020 Statement by William Evanina, Director of the National Counterintelligence and Security Center:

"During this time of unexpected challenges to our nation as a result of COVID-19, we are acutely aware of the potential for economic hardship on security clearance holders. It is imperative that we ensure trusted security clearance holders, or applicants, who may suffer financial hardship as a result of the virus, are not unduly penalized because of circumstances beyond their control. With the implementation of 'Trusted Workforce 2.0,' and the incorporation of Continuous Evaluation (CE), we are committed to our 'Whole Person Concept' approach when vetting personnel for positions of trust.

"Hence, I want to emphasize and call attention to mitigating factors which are contained in Security Executive Agent Directive 4 (SEAD 4) Guideline F; Financial Considerations: *(b) the conditions that resulted in the financial problem were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, a death, divorce or separation, clear victimization by predatory lending practices, or identity theft), and the individual acted responsibly under the circumstances.*

"I will notify Departments and Agencies for their attention to mitigating condition (b) listed above. This guidance applies not only to existing clearance holders, but also to applicants being processed for initial security clearances."

Sheltering at Home

By Jim Fredette, ISSA-COS, March 30, 2020

As a result of the COVID-19 health crisis and in compliance with the Amended Public Health Order 20-24 Implementing Stay at Home Requirements many of us are working from home. This work from home idea is actually a new thing for many of us. Staying gainfully employed without physically working on our systems taxes our imaginations. So how do we stay busy and provide benefit for our cyber requirements while providing our employer with bang for their buck? After all, we need to pickup again when this is all over and probably way behind on our normal day to day efforts.

First of all, look at this as an opportunity to accomplish those administrative tasks that always get pushed to the bottom of the list. Now is a great time to review and update those policies, plans and procedures. Even if they are perfect, annual reviews are still required. Don't forget to document this action so you can provide that proof to management and inspectors. While you are doing your review, make sure you address any lessons learned from all this remote work. Especially any issues you may have seen in VPN capabilities and network overhead.

Next, look at your user training and management reports. In most cases they could use improvement but never get addressed. Again, don't forget to address any lessons learned from working remote. It is also an opportunity to do some online training and webinars which provide those precious CEU/CPEs. So, for example if you are working on updating your Incident Response Plan (IRP), spend some time accomplishing some IRP education yourself.

Finally, take advantage of the break from everyday and do some tabletop exercises to validate your cyber practices. You can run the exercise with Skype, Microsoft Team, or another meeting application if available. Otherwise, email between you and the key personnel can still work. Don't forget to document the exercise and your lessons learned.

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**

UCCS receives $6 million Department of Labor grant to implement cybersecurity apprenticeships

By Staff, UCCS, February 26,2020

A nearly $6 million grant from the U.S. Department of Labor will fund the Colorado Cybersecurity Apprenticeship Program, or C-CAP, to train workers for mid-level and advance-level cybersecurity roles. The program will be administered through the UCCS College of Business for the next four years.

"The grant enables us to serve communities in 10 states with high demand for skilled cybersecurity professionals, particularly California, Colorado, Florida, Texas and Virginia," said Gurvirender Tejay, associate professor of information systems and director of C-CAP. "We look forward to partnering with employers, workforce development boards, community colleges and relevant communityorganizations to expand the program nationwide. UCCS is a leader in cybersecurity education and through C-CAP will serve to address severe cybersecurity skills gap facing our nation."

C-CAP will include five cybersecurity apprenticeship programs to align with industry needs for analysts, consultants, IT auditors, penetration and vulnerability testers, and managers. Each program will require the completion of three courses and associated bootcamps for a total of 12 credit hours of college education that will bridge the gap between basic and mid-level cybersecurity skills.

Each student will receive a mentor in the cybersecurity industry to guide and support their progression through the apprenticeship through the College of Business' Relationships, Opportunity, Acumen and Readiness, or ROAR, program. Participating companies have agreed to provide salary increases to students in the program as they complete milestones and courses can be completed online to support the hands-on training at the company's location.

Students who complete the program will receive a minor in cybersecurity, a certificate in cybersecurity management and be eligible to take one of 10 industry-recognized certifications: CISM, CRISC, CEH, CISA, CySA+, SSCP, GCIH, GCIA, CCS and CCSP. It is expected that more than 5,100 students will be able to complete the program during the next four years.

"We are excited to be facilitating a collaboration between employers and students that brings 21 century cybersecurity skills to the workplace," said Robert Block, associate dean of the College of Business and associate professor of business analysis, and co-director of C-CAP. "We look forward to creating a competitive highly skilled cybersecurity workforce made up veterans, military spouses, underemployed workers, minorities and women."

The grant to UCCS was part of a nearly $100 million allocation to 27 organizations across the country. The $5,996,713 award to UCCS was the second largest to a university, behind North Carolina State University. It was made in response to the executive order "Expanding Apprenticeship in America" signed by President Donald J. Trump June 15, 2017.

"These grants will further the administration's efforts to expand apprenticeships," said Eugene Scalia, U.S. Secretary of Labor. "Companies across the country tell me that their greatest challenge today is finding the skilled workers they need. This funding will bolster America's competitiveness by adding more skilled workers to fill millions of open jobs today and in the future."

For more information on C-CAP, contact Tejay at gtejay@uccs.edu.

The UCCS College of Business was established in 1965 and has more than 1,300 undergraduates and 350 MBA and distance MBA students. The College of Business and Administration awards the Bachelor of Science in Business and Bachelor of Innovation degrees. The Graduate School of Business Administration awards the Master of Business Administration and Master of Science in Accounting degrees. More than 10,000 alumni of the College of Business live and work around the world. For more information, visit uccs.edu/business.

The University of Colorado Colorado Springs offers 50 bachelor's, 24 master's and seven doctoral degree programs. UCCS enrolls about 12,000 students on campus annually. For more information, visit uccs.edu.

Why All Employees Are Responsible for Company Cybersecurity

By Diya Jolly, DarkReading, April 1, 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.

The Equifax breach serves as a stark example of how seemingly benign or minute employee decisions (such as using an easily hacked password or opening a suspicious attachment in an email) can have significant consequences. Weak or stolen passwords cause 81% of data breaches, which indicates our identities — and particularly our login credentials — are highly valuable corporate assets that hackers actively target.

Lax security behavior isn't just dangerous to the company you work for — it can pose significant personal risks as well. When one of your employees makes their company's data vulnerable, they might also be exposing their own sensitive information, like Social Security and credit card numbers. Overall, human error causes a staggering 90% of data breaches, so it's critical you make sure every employee is aware of the risks they pose so they can take active steps to improve security at work. Ideally, your company should have stringent security and identity management policies in place to protect sensitive information and data. But beyond that, here's what you should be encouraging all employees to do:

Be Smart When Working Outside the Office

Experts anticipate the bring-your-own-device market will be worth over $366 billion by 2022 (compared with $30 billion in 2014), which means increasing numbers of employees are doing work on their personal laptops and smartphones. Lots of factors contribute to this trend, including the ubiquity of public Wi-Fi. Working from personal devices and taking advantage of public Wi-Fi networks gives you a significant amount of flexibility, allowing you to send emails from the checkout aisle at the grocery store or work on a report at a café in between meetings.

However, while convenient, doing work on public Wi-Fi networks and personal devices can be risky. Hackers can get access to an employee's personal data by intercepting the information they send or access over the Wi-Fi network. Hackers are also taking advantage of the fact that people like to do work on personal devices such as iPhones. Malware attacks on smartphones rose by 50% between 2018 and 2019, and something as simple as downloading an illegitimate app or failing to update your operating system could expose a mobile device to malware.

Research shows 31% of data breaches lead to employees getting fired, so if your employees are using a personal device or unsecured Wi-Fi network to do work, here are a few things they can do to protect their data:

- Make sure they are only downloading legitimate, supported apps.
- Set up two-factor authentication for any app that offers it.
- Use a strong passcode and biometric authentication (such as fingerprint or face scan) to unlock devices, when available.
- If they want to use an app that requires or allows for social authentication (such as Facebook Login), double-check what the authenticator shares with other parties. Otherwise, they could unintentionally expose corporate information through Facebook authentication.

Don't Trust Just Your Password to Protect You

The goal for many companies is to "go passwordless," only requiring users to log in to company apps with a variety of factors such as magic links and biometric identifiers, instead of relying on passwords. Ideally, your company should be implementing multifactor authentication and using technology that allows for single sign-on to limit the number of passwords you're expected to manage. But if your organization still requires passwords, encourage your employees to take their personal security a step further by using a password manager. The goal here is for them to make their passwords so complex, not even they know them. Password managers abound with a range of features to suit just about every use case.

Read the rest here:

https://www.darkreading.com/vulnerabilities---threats/why-all-employees-are-responsible-for-company-cybersecurity/a/d-id/1337401

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.

Additional details will follow as they become available.

2020 ISSA Awards Program

ISSA annually recognizes outstanding information security professionals, their companies, and chapters that are at the top of their respective games. Who would you like to see recognized? Nominations may be made by any member. Anyone interested in making a nomination should thoroughly review the 2020 Awards Policies and Procedures once they are available.

This year's awards will be presented at the ISSA International Summit. Award winners will receive transportation, lodging, and complimentary registration. Any member in good standing is eligible to propose candidates in all categories.

In 2019 the ISSA International presented awards in these categories:

Hall of Fame: pays homage to an individual's exceptional qualities of leadership in his or her own career and organization as well as an exemplary commitment to the information security profession (ISSA membership not required).

Honor Roll: recognizes an individual's sustained contributions to the information security community, enhancement of the professionalism of ISSA members, and advancement of the association.

Security Professional of the Year: honors the member who best exemplifies the most outstanding standards and achievement in information security in the preceding year.

Volunteers of the Year: recognizes members who have made a significant difference to his or her chapter, the association, or the information security community through dedicated and selfless service to ISSA.

Chapters of the Year: rewards chapters that have done an exceptional job of supporting ISSA's mission, serving their member communities, and advancing the field. Nominees will be evaluated on their activities and programs in six areas: member services, membership development, projects and special events, development of the next generation of security professionals, communications and marketing, and participation and support of ISSA International initiatives and programs.

There are four chapter categories available for nomination:

- Small: Less than 100 members
- Medium: 100-300 members
- Large: More than 300 members
- International: Non-US Chapter (new in 2018)

Organization of the Year: acknowledges an organization that has provided a sustained, proactive presence that directly contributed to the overall good and professionalism of the association and its membership, providing services, products, and/or direct support that ensures the promotion of the highest ethical standards in addressing information security and its future direction.

President's Award for Public Service: honors an individual's contribution to the information security profession in the area of public service. (ISSA membership not required).

The 2020 Award criteria will be made available soon and will be in the chapter newsletter.

The Internet of Things is a security nightmare reveals latest real-world analysis: unencrypted traffic, network crossover, vulnerable OSes

And the best part of it? Hospitals are most at risk

By Kieren McCarthy, The Register, March 11, 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.

What's more, most networks mix IoT devices with more traditional IT assets like laptops, desktops and mobile devices, exposing those networks to malware from both ends: a vulnerable IoT device can infect PCs; and an unpatched laptop could give an attacker access to IoT devices - and vast quantities of saleable data.

Those are the big conclusions from a real-world test of 1.2 million IoT devices across thousands of physical locations in the United States, carried out by Palo Alto Networks.

The company also focused in on the healthcare industry and found a truly alarming security situation: no less than 83 per cent of medical imaging devices run on unsupported operating systems; a massive 56 per cent jump from two years ago because of the end of support for Windows 7.

That leaves hospitals "vulnerable to attacks that can disrupt care or expose sensitive medical information," the report notes. In addition, 72 per cent of healthcare VLANs mix IoT and traditional assets, so the potential for hackers to access personal health data is a ticking time bomb.

The researchers estimate that more than half - 57 per cent - of IoT devices are currently vulnerable to medium or high-severity attacks, making them an obvious target for hackers. "We found that, while the vulnerability of IoT devices make them easy targets, they are most often used as a stepping stone for lateral movement to attack other systems on the network," the report noted. "Furthermore, we found password-related attacks continue to be prevalent on IoT devices due to weak manufacturer-set passwords and poor password security practices."

Hate to say everyone told you so...

In short, the poor IoT security that people have been warning about for years now risks compromising larger networks because they are being attached to the same network; and thanks to a failure to upgrade imaging equipment to newer operating systems, hackers also have an extra route in networks where they could gather vast amounts of data from unencrypted IoT devices. A double-whammy in other words.

There is a small amount of good news: California's new IoT law (SB-327) that requires a different password for every device - rather than manufacturer defaults - came into effect at the start of the year and is expected to cut down on easy hacks.

While that is an improvement, as we previously noted the law only deals with the lowest hanging fruit and did not include things like secure software updates which are, over time, a greater security risk - as those running Windows 7 are likely to find out over the next few years. Even a law requiring manufacturers to periodically prompt users to upgrade their software could have a massively positive security impact.

Laws requiring encryption would also be a huge help. As would a data-minimization law that requires companies to only request and store data that is needed for the functioning of their products. As would some kind of compulsory two-factor authentication.

The fear is that lawmakers will take their focus off terrible IoT security now that they passed a law eliminating default passwords. As far as we are aware, that appears to be playing out with no new security legislation working its way through the corridors of power.

Read the rest here:

https://www.theregister.co.uk/2020/03/11/the_internet_of_things_is_a_security_nightmare_reveals_latest_realworld_analysis_unencrypted_traffic_network_crossover_vulnerable_oses/?&web_view=true

Working from home? Here are the steps all workers and companies should take to avoid cyberattacks, according to experts

By Aaron Holmes, Business Insider, March 16, 2020

For workers being instructed to work from home amid the COVID-19 outbreak, doing jobs remotely can be a major adjustment. For hackers, it can be an opportunity.

Remote work means a rise in the number of devices employees are using for their jobs, and an increase in the use of online conferencing tools like Zoom, Google Hangouts, Microsoft Teams, and Slack. That shift also give hackers a larger number of potential targets.

Cybersecurity research firms are predicting a spike in hacks and breaches targeting businesses as the COVID-19 outbreak continues, Business Insider's Jeff Elder reported last week. The Department of Homeland Security has also advised businesses to prepare for new cybersecurity threats arising from work-from-home arrangements.

Business Insider asked cybersecurity experts about measures workers and companies can take to significantly reduce their vulnerability while working from home. Here's what they recommend.

Companies should make sure their workers are up to speed on basic security hygiene, including strong passwords and multifactor authentication.

"With a remote workforce and everybody working digitally, the threat landscape certainly increases," said Kiersten Todt, managing director of the Cyber Readiness Institute and former cybersecurity adviser to the Obama administration. "Now's a really good time to look at all the capabilities you could be using, like multifactor authentication, and to turn them on."

Workers should be especially wary of suspicious emails and avoid clicking on links that are new or unfamiliar to them.

Hackers are already running phishing scams that capitalize on COVID-19 fears, posing as health authorities to get people to click on malicious links.

"For now, individuals are going to be a lot more targeted because they know there's going to be a path to company assets," said Stephen Breidenbach, co-chair of the cybersecurity practice at the law firm Moritt Hock & Hamroff. "I would not be surprised to see an attacker posing as tech support targeting the employee who is outside of the office now."

As a general rule, never share personal or financial information via email or message.

Most phishing schemes aim to extract people's personal information or login credentials as quickly as possible. If you think someone at your company is asking for your personal information, call them to confirm, and if necessary, give them the information via phone.

Before circulating or acting on news about COVID-19 and its impact on your business, verify that it's coming from a trusted source.

Read the rest here:

https://www.yahoo.com/news/working-home-steps-workers-companies-163948072.html

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 Schedule of Events

Chapter Meetings – Dinner (5:30 – 7:30 PM)
Tuesday, May 19, 2020
Tuesday, July 21, 2020
Tuesday, August 18, 2020
Tuesday, October 20, 2020
Tuesday, November 17, 2020

Chapter Meetings – Lunch (11:00 – 1:00 PM)
Wednesday, May 20, 2020
Wednesday, July 22, 2020
Wednesday, August 19, 2020
Wednesday, October 21, 2020
Wednesday, November 18, 2020

Mini-Seminars – Breakfast (8:30 – 12:00 PM)
Saturday, May 16, 2020
Saturday, July 25, 2020
Saturday, August 22, 2020
Saturday, October 24, 2020
Saturday, November 14, 2020

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

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

See Pages 20 and 21 for online presentations!

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

OMB to Agencies: Time to Finish IPv6 Transition

By Aaron Boyd, NextGov, March 2, 2020

With the 2021 budget proposal in the rearview, the Office of Management and Budget's IT policy shop released its first new guidance of the calendar year: a final push on getting agencies transitioned to IPv6, the current standard for identifying systems and devices communicating with and over the internet.

The previous standard, IPv4, created addresses using a 32-bit format, capping the total number of addresses at 2^32, or just shy of 4.3 billion. The IPv6 schema is 128-bit, enabling more than 340 undecillion, or 340,000,000,000,000,000,000,000,000,000,000,000,000 addresses.

The shift to IPv6 adds significantly more addresses to the global pool, as well as a different numbering format. While IPv4 shows addresses as four sets of one to three digits, IPv6 uses eight sets of four digits. For organizations—including federal agencies—the new format requires recoding systems that run network infrastructure to understand and ingest IPv6 addresses.

Introducing the memo in a notice posted Monday on the Federal Register, Federal Chief Information Officer Suzette Kent cited increased adoption in the private sector over the last five years.

"Mobile networks, data centers and leading-edge enterprise networks, for example, have been evolving to IPv6-only networks," she said. "It is essential for the federal government to expand and enhance its strategic commitment to the transition to IPv6 in order to keep pace with and capitalize on industry trends."

The new draft guidance issued Monday requires agencies to develop and implement plans to ensure "at least 80% of IP-enabled assets on federal networks are IPv6-only by the end of fiscal 2025," with lower targets to hit in fiscal 2023 and 2024.

Read the rest here:

https://www.nextgov.com/it-modernization/2020/03/omb-ipv6-transition/163459/

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.

Strategic Partnership – NCX

CyberAlliance+

www.nationalcyber.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

April Online Presentations

04/09/2020

- **Speaker: Mr. Wally Magda**
- **Title: How do you keep the lights on and the gears turning during a global pandemic?**

04/16/2020

Speaker: Dr. Erik Huffman

Title: Psyberscurity… *not a typo!*

04/23/2020

- **Speaker: TBD**
- **Title: TBD**

04/30/2020

- **Speaker: TBD**
- **Title: TBD**

ISSA
Information Systems Security Association
Colorado Springs Chapter

ISSA-COS Online Series – Session 2

Date: April 9, 2020, 6 – 7:30 PM

Guest Speaker: Mr. Wally Magda, CEO | Owner, WallyDotBiz, LLC

Title: How do you keep the lights on and the gears turning during a global pandemic?

Synopsis: ICS/SCADA critical infrastructure is "insecure by design." It was designed to work; it was not designed to be secure!! In addition to threat actors, ransomware and bots, what is the impact of pandemic stress on your systems? What about your supply chain? What is your resilience against disruption to the availability of critical components, materials, and support resources with supply chains originating in or traversing significantly impacted regions globally. What about your people? Remote access plays a key part in keeping the gears turning and keeping the lights on. However, even with all the automation, remote control can only go so far. Oh my!!! You just learned that a cryptographic key utilized to protect the account password is hard coded into the programs running on your control devices. An attacker can easily use that information to launch ransomware and bring you down. The vulnerability rating severity is a 10-CRITICAL. You can't patch that remotely! Now what do you do?

Register at: www.issa-cos.org

ISSA
Information Systems Security Association
Colorado Springs Chapter

ISSA-COS Online Series – Session 3

Date: April 16, 2020 6 – 7:30 PM
Guest Speaker: Dr. Erik Huffman
CEO/Founder, Handshake Leadership

Title: Psyberscurity (No typo)

Synopsis: Cybersecurity is the combination of technology, organizational operations, people, and culture. This talk specifically address issues residing in the sociological impacts in cybersecurity. Dr. Huffman is a cybersecurity researcher in the emerging field of cyberpsychology; the combination of cybersecurity and psychology. His research has led him into the exploration of the effectiveness of cybersecurity training. It has been said that we need to train how we fight. What happens when we actually do that?

Register at: www.issa-cos.org

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

A German Army Laptop Sold for €90 on eBay – With Military Secrets

By Conor Reynolds, CBR, March 18, 2020

A decommissioned German army laptop sold on eBay for €90 contained classified military data, including ways to defeat a mobile air defense system in use today.

The laptop was bought from IT recycling firm Bingen by G Data, a prominent German software security firm, which detailed the incident in a March 16 blog.

Worryingly for the Bundeswehr, not only did it contain sensitive information, but administrative software was protected with the robust password "guest". (The laptop itself, running the obsolete Windows 2000, was not password-protected).

Read the rest here:

https://www.cbronline.com/news/german-army-laptop-secrets

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