November 10th, 2020

Try our November - 'Phishing' Quiz

This week's stories:

- Canadian Institutions Join Fortinet's Security Academy Program to Address Cybersecurity Skills Gap
- 2 hard drives and documents with personal health info left behind during MLHU move
- Cianfarani: Canada should rely more on its own cyber-security industry
- FTC Requires Zoom to Enhance its Security Practices as Part of Settlement
- New ESET/NCSA Survey Explores the Internet of (Stranger) Things
- Fake Microsoft Teams updates lead to Cobalt Strike deployment
- FBI: Hackers stole source code from US government agencies and private companies
- North Korea attacks targeting defense workers more covert than previously thought
- Luxottica data breach exposes LensCrafters, EyeMed patient info
- FBI is investigating more than 1,000 cases of Chinese theft of US technology
- RansomExx ransomware also encrypts Linux systems
- San Diego Can't Actually Turn Its Smart Streetlights Off

Canadian Institutions Join Fortinet's Security Academy Program to Address Cybersecurity Skills Gap

https://markets.businessinsider.com/news/stocks/canadian-institutions-join-fortinet-s-security-academy-program-to-address-cybersecurity-skills-gap-1029781585

"The cybersecurity skills gap affects businesses and governments across Canada, and ultimately impacts our digital economy. Fortinet is investing heavily in training and education through our NSE Training Institute to create more career pathways in Canada and globally. Fortinet is partnering with Canadian academic institutions and veteran-focused nonprofits to extend our reach and develop a stronger pipeline of security professionals."

Click link above to read more

---

2 hard drives and documents with personal health info left behind during MLHU move

https://london.ctvnews.ca/2-hard-drives-and-documents-with-personal-health-info-left-behind-during-mlhu-move-1.5179108

LONDON, ONT. -- The Middlesex-London Health Unit (MLHU) is defending itself over a privacy breach earlier this year when papers and two computer hard drives containing personal information and personal health information were left behind at its former headquarters on King Street.

Click link above to read more

Cianfarani: Canada should rely more on its own cyber-security industry

https://ottawacitizen.com/opinion/cianfarani-canada-should-rely-more-on-its-own-cyber-security-industry

When Spanish Flu hit at the end of the First World War, the telephone was just coming into widespread use. Its impact on the pandemic was marginal. Today, by contrast, as countries around the world battle COVID-19, communications technologies have become as essential as that Zoom call with grandma you've been having on Sundays. The past eight months have transformed businesses, governments and homes into cyber dependencies.

Click link above to read more

FTC Requires Zoom to Enhance its Security Practices as Part of Settlement

https://www.ftc.gov/news-events/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement

The Federal Trade Commission today announced a settlement with Zoom Video Communications, Inc. that will require the company to implement a robust information security program to settle allegations that the video conferencing provider engaged in a series of deceptive and unfair practices that undermined the security of its users.

Zoom has agreed to a requirement to establish and implement a comprehensive security program, a prohibition on privacy and security misrepresentations, and other detailed and specific relief to protect its user base, which has skyrocketed from 10 million in December 2019 to 300 million in April 2020 during the COVID-19 pandemic.

Click link above to read more

New ESET/NCSA Survey Explores the Internet of (Stranger) Things

https://www.eset.com/ca/about/newsroom/corporate-blog/survey-internet-of-stranger-things0/

Today, ESET and the National Cyber Security Alliance jointly released survey results that reveal the unease with which people approach our increasingly digitally connected lives. Internet-connected home appliances, toys, automobiles and a myriad of smart-gadgets certainly open up new possibilities. But do they also expose a portal to more insidious forces?

Consider some of these survey highlights as daily life comes face-to-face with the unknown.

Click link above to read more

Fake Microsoft Teams updates lead to Cobalt Strike deployment

https://www.bleepingcomputer.com/news/security/fake-microsoft-teams-updates-lead-to-cobalt-strike-deployment/

Ransomware operators are using malicious fake ads for Microsoft Teams updates to infect systems with backdoors that deployed Cobalt Strike to compromise the rest of the network.

The attacks target organizations in various industries, but recent ones focused on the education sector (K-12), which depends on videoconferencing solutions due to Covid-19 restrictions.

Click link above to read more

FBI: Hackers stole source code from US government agencies and private companies

https://www.zdnet.com/article/fbi-hackers-stole-source-code-from-us-government-agencies-and-private-companies/

The Federal Bureau of Investigation has sent out a security alert warning that threat actors are abusing misconfigured SonarQube applications to access and steal source code repositories from US government agencies and private businesses.

Intrusions have taken place since at least April 2020, the FBI said in an alert sent out last month and made public this week on its website.

Click link above to read more

North Korea attacks targeting defense workers more covert than previously thought

https://www.scmagazine.com/home/security-news/north-korea-attacks-targeting-defense-workers-more-covert-than-previously-thought/

McAfee researchers announced Thursday that an espionage campaign targeting defense and aerospace contractors using job offers on LinkedIn covered a broader geographic area than previously thought.

The campaign, called Operation North Star, was first reported by McAfee over the summer. The attacks showed similar tactics, techniques and procedures to the North Korean actor Hidden Cobra and targeted South Korean firms. The campaign phished employees by copying job opportunities from legitimate websites and crafting lures that were diligently tailored to the targets.

Click link above to read more

Luxottica data breach exposes LensCrafters, EyeMed patient info

https://www.bleepingcomputer.com/news/security/luxottica-data-breach-exposes-lenscrafters-eyemed-patient-info/

A Luxottica data breach has exposed the personal and protected health information for patients of LensCrafters, Target Optical, EyeMed, and other eye care practices.

Luxottica is the world's largest eyewear company with a portfolio of well-known eyeglass brands, including Ray-Ban, Oakley, Oliver Peoples, Ferrari, Michael Kors, Bulgari, Armani, Prada, Chanel, and Coach.

In addition to selling eyeglasses, Luxottica also operates the EyeMed vision benefits company and partners with eye care professionals as part of their LensCrafters, Target Optical, EyeMed, and Pearle Vision retail outlets

Click link above to read more

FBI is investigating more than 1,000 cases of Chinese theft of US technology

https://www.zdnet.com/article/fbi-is-investigating-more-than-1000-cases-of-chinese-theft-of-us-technology/

Members of the US government held a conference in Washington this week on the topic of Chinese theft of intellectual property from US technology firms and the US academic sector.

Officials said the purpose of the conference -- named the China Initiative Conference -- was to bring the US private sector and the academic and research communities up to speed with the US government's investigations.

Click link above to read more

RansomExx ransomware also encrypts Linux systems

https://www.bleepingcomputer.com/news/security/ransomexx-ransomware-also-encrypts-linux-systems/

With companies commonly using a mixed environment of Windows and Linux servers, ransomware operations have increasingly started to create Linux versions of their malware to ensure they encrypt all critical data.

A new report today by Kaspersky takes a look at the Linux version of the RansomExx ransomware, also known as Defray777.

RansomExx has been getting a lot of attention this week due to their ongoing attacks against Brazil's government networks and previous attacks against the Texas Department of Transportation, (TxDOT), Konica Minolta, IPG Photonics, and Tyler Technologies.

Click link above to read more

San Diego Can’t Actually Turn Its Smart Streetlights Off

https://www.voiceofsandiego.org/topics/public-safety/san-diego-cant-actually-turn-its-smart-streetlights-off/

The San Diego Police Department stopped using the city’s smart streetlights last month, but the cameras are still on — and still recording.

After the City Council blocked funding for the controversial program this summer, Mayor Kevin Faulconer ordered his staff to cut off access to the network. He was responding to criticism from both elected officials and activists who’ve been advocating for a surveillance ordinance and privacy advisory commission.

Click link above to read more

---

http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest

To learn more about information security issues and best practices, visit us at:

https://www.gov.bc.ca/informationsecurity
OCIOSecurity@gov.bc.ca