February 16th, 2021

Try our February "LOVE SECURITY" Quiz

This week's stories:

IBM hands out $3M in cybersecurity funding for U.S. public schools

For years, schools have been fighting an uphill battle when it comes to cybersecurity. The COVID-19 pandemic has only made it worse as they become key targets for hackers as millions of teachers and students have turned to video chat software and other online tools for remote learning.

IBM is awarding grants totalling $3 million in value to help six public school districts in the United States prepare for and respond to cyberattacks. The grants are for U.S. public schools only.

"Unfortunately at this time the program is only in the U.S. We do have other programs in play in Canada, but not this specific one," Lorraine Baldwin, external communications leader for IBM Canada, told *IT World Canada* in an email.

https://www.itworldcanada.com/article/ibm-hands-out-3m-in-cybersecurity-funding-for-u-s-public-schools/442196

Click link above to read more

'Cyber security incident': Participants in Mississauga climate survey have email addresses stolen

Participants of a City of Mississauga climate survey have had their email addresses stolen in a cyber breach involving a contractor working for the city.

The emails were collected as part of a survey for the city's climate change action plan that was live from Sept. 29 to Oct. 20, 2020 and accessed in a "cyber security incident" early this year at National Public Relations, the contractor working for Mississauga.

"We have conducted a thorough investigation of the matter and can confirm that only the email addresses and usernames of survey participants that opted to provide their emails for a prize draw were accessed," said Gillian Smith, a managing partner at National. "We held no other personal information of survey participants."

Online scammers can use emails and other personal information in attempts to defraud potential victims.

The city said it became aware of the security breach Jan. 20 and in a Feb. 9 email disclosing the incident, Mississauga advised that participants "be vigilant and exercise caution regarding the email address that you used for the survey."

https://www.mississauga.com/news-story/10329390--cyber-security-incident-participants-in-mississauga-climate-survey-have-email-addresses-stolen/

Click link above to read more

Why A Zero-Trust Policy Is Important For Remote Companies And Cybersecurity Effectiveness

More than a lack of resources, cybersecurity seems to suffer from a lack of an effective approach, especially as the face of work is changing. The emergence of remote work as the norm for many companies comes with new cybersecurity challenges. Remote working results in less control over the organization's resources, which heightens the risk of data breaches. It is, therefore, more important than ever to approach cybersecurity from a risk-based perspective.

The zero-trust idea has been gradually gaining momentum over the years, especially with the rise of SaaS and remote work. It has also become more practicable as technologies and tools built on its framework become mainstream. Zero trust is rooted in the belief that nothing should be trusted, whether it resides within the network or without. Instead, always verify.

https://www.forbes.com/sites/forbestechcouncil/2021/02/12/why-a-zero-trust-policy-is-important-for-remote-companies-and-cybersecurity-effectiveness/?sh=2f39466820f5

Click link above to read more

Washington auditor's office warned agencies of data-breach risks. Then it got hacked

On Christmas Eve last year, Washington State Auditor Pat McCarthy's office issued a dire warning that state agency computer systems and data make "attractive targets for cyberattacks."

The admonition, in a 26-page cybersecurity audit report titled Continuing Opportunities to Improve State IT Security, noted agencies collect "vast amounts of confidential data" from the public.

It recommended fixes for "vulnerabilities" at five unnamed state agencies, cautioning — presciently, as it turned out — that a sensitive-data breach would bring a "loss of public confidence" as well as "considerable tangible costs."

The next day, Christmas, unknown actors compromised the auditor's own computer files, exposing a vast trove of private information in what may be the largest-ever cyberbreach for a Washington state agency.

The data included driver's license, Social Security and bank account numbers of more than 1.4 million unemployment claimants. It also included audit data involving 25 state agencies and 100 local governments, including the city of Seattle, as well as adoption files of 30 children and their families.

https://www.seattletimes.com/seattle-news/politics/washington-auditors-office-warned-agencies-of-data-breach-risks-then-it-got-hacked/

Click link above to read more

Cybersecurity spending for critical infrastructure to reach $105.99 billion in 2021

Cybersecurity spending in critical infrastructure has been little impacted by the COVID-19 pandemic, save for some reshuffling on where that spend is most needed. The effect has been mostly in increased demand for secure remote connectivity.

Most of the cybersecurity spending announced by governments has not changed significantly however, with most maintaining similar funding planned in previous years, with an average Year-on-Year growth rate between 5% and 10%.

According to a report by ABI Research, cybersecurity spending for critical infrastructure (CI) will increase by $9 billion over the next year to reach $105.99 billion in 2021.

Secure connectivity has become a key focus

The primary challenge of the COVID-19 pandemic has been for CI operators to ensure that systems and services keep running smoothly, despite an increasingly remote workforce. As such, greater emphasis has been placed on ensuring that infrastructure operations can be securely monitored and managed remotely by authorized personnel.

https://www.helpnetsecurity.com/2021/02/16/cybersecurity-spending-critical-infrastructure/

Click link above to read more

Fraud Continues to Grow for Financial Services: How to Avoid Financial Advisor Scams

During these financially destabilizing times, you may have reached out to a financial advisor for help navigating this difficult economy. Seeking a financial expert's advice is one of the most common methods people use to protect themselves from financial scams. However, what happens when the person you are turning to for advice is an unscrupulous figure who is engaging in fraudulent behavior? It is important to understand how fraud works in the financial services industry so that you can take steps to protect yourself.

What Is a Financial Advisor Scam?

Financial advisor scams occur when a person you trust as your fiduciary gives you self-serving financial advice that may not be appropriate for you and is more interested in helping the advisor than you.
A study by the FINRA Investor Education Foundation found that 80% of American investors had been solicited to participate in a fraud scheme and 11% of American investors reported they had lost money to a fraud scheme. However, researchers note that victims of financial advisor scams are often too embarrassed to come forward, so these numbers may be underreported.

https://www.globalbankingandfinance.com/fraud-continues-to-grow-for-financial-services-how-to-avoid-financial-advisor-scams/

Click link above to read more

Effects of Cybercrime in Developing Economies: How Cyber Law Can Help

Cybercrimes are a broad range of criminal activities that involve computers, computer networks, or networked devices. Cybercrime encompasses computer fraud, phishing scams, theft of trade secrets or corporate data, ransomware attacks, cyber espionage, identity theft, and many other crimes. Cybercrimes can result in the loss of funds, identities, and other resources. Those that target people in developing countries can cause the most harm.

Cyber laws counteract this criminal activity, investigating and prosecuting cybercriminals. Read on to learn more about the role of cyber law and how it can help countries with developing economies.

https://techlog360.com/effects-of-cybercrime-in-developing-economies/

Click link above to read more

---

7 Ways To Prepare For And Recover From Cyber Attack Crisis Situations

On Tuesday, the FBI's Cyber Division issued a warning to businesses and law enforcement agencies about potential computer vulnerabilities that led to the February 5 hacking of a water treatment plant in Oldsmar, Florida.

The event was the latest headline-making reminder for business leaders about the dangers of assuming their companies are immune from an increasingly common type of crisis—cyber attacks. These attacks threaten the ability of organizations to protect their data, the privacy of customers, and conduct day-to-day business operations.

The Importance of Full Disclosure

The failure to notify those who are affected by the crisis—including customers, employees, and the public — can create another crisis for companies. Full and immediate disclosure of cyber attacks is an important crisis management best practice.

https://www.forbes.com/sites/edwardsegal/2021/02/12/7-ways-to-prepare-for-and-recover-from-cyber-attack-crisis-situations/?sh=5a1e7d3a47dc

Click link above to read more

France: Russian state hackers targeted Centreon servers in years-long campaign

France's cyber-security agency said that a group of Russian military hackers, known as the Sandworm group, have been behind a three-years-long operation during which they breached the internal networks of several French entities running the Centreon IT monitoring software.

The attacks were detailed in a technical report released today by Agence Nationale de la Sécurité des Systèmes d'Information, also known as ANSSI, the country's main cyber-security agency.

"This campaign mostly affected information technology providers, especially web hosting providers," ANSSI officials said today.

"The first victim seems to have been compromised from late 2017. The campaign lasted until 2020."

https://www.zdnet.com/article/france-russian-state-hackers-targeted-centreon-servers-in-years-long-campaign/

Click link above to read more

‘Privacy More Imp Than Money’: SC Issues Notice in WhatsApp Case

Supreme Court, on Monday, 15 February, issued a notice on an application seeking to restrain WhatsApp from implementing its new privacy policy in India. The plea pointed out the ‘different’ privacy policy, which is made applicable to users in Europe, LiveLaw reported, and suggested the same be applied to India.

"The privacy of people is more important than your money," remarked Chief Justice of India SA Bobde while issuing notices to Facebook and WhatsApp on an application seeking to restrain WhatsApp from implementing its new privacy policy in India.

According to the LiveLaw report, the CJI observed that people have grave concerns about their right to privacy with respect to Whatsapp's new policy.

Following the hearing, the Constitutional Bench directed the company to explain its stance by filing a counter affidavit within four weeks, on the application that was filed by the Internet Freedom Foundation (IFF).

WhatsApp head, Will Cathart had clarified last month that the recent privacy policy update 'does not change WhatsApp's data-sharing practices with Facebook'.

https://ca.news.yahoo.com/privacy-more-imp-money-sc-082353151.html

Click link above to read more

Ransomware attack spike targets hospitals

An uptick in ransomware complaints flooded the FBI in the final months of 2020, including a spate of attacks on hospitals, The Washington Times has learned.

In each of the last four months of 2020, the FBI received more than 200 complaints about ransomware, according to data compiled by the FBI's Internet Crime Complaint Center that was shared with The Times.

Victims' cash losses more than tripled in 2020 year over year to $29.1 million, according to data collected by the FBI.

The complaints peaked in October with 302 reports of ransomware, which is malicious software that infects a computer system and threatens to publish the victim's data or block access to it unless a ransom is paid.

The rest of 2020 had just two months with 200 ransomware complaints to the FBI, according to the data, which does not capture unreported ransomware attacks.

https://www.washingtontimes.com/news/2021/feb/14/ransomware-attack-spike-targets-hospitals/

Click link above to read more

Top 5 security risks to connected cars, according to Trend Micro

Analysts from Trend Micro rate DDoS attacks and electronic jamming as some of the highest cybersecurity risks for connected cars.

A new report from Trend Micro analyzes a day in the travels of a connected car to identify the cyberattacks most likely to succeed. "Cybersecurity for Connected Cars: Exploring Risks in 5G, Cloud and Other Connected Technologies" puts the overall risk at medium. Among the millions of endpoints in a connected car's ecosystem, analysts found 29 potential cybersecurity attack vectors and ranked five as the highest risks.

Connected cars use satellite, cellular, Wi-Fi, Bluetooth, RDS, eSIM-based telematics, and other types of connectivity to send and receive data; this data supports user applications, driving applications, autonomous driving, safety features, and other activities. The authors note that all these network-centric applications create new attack surfaces in connected cars. Another element of the overall security challenge is a connected car's interactions with other vehicles, cloud services, and road infrastructure.

https://www.techrepublic.com/article/top-5-security-risks-to-connected-cars-according-to-trend-micro/?ftag=TREa988f1c&bhid=42420269&mid=13269630&cid=2176068089

Click link above to read more

Singtel Supply Chain Breach Traced to Unpatched Bug

One of APAC's biggest telecoms companies has admitted that a supply chain attack may have led to the compromise of customer data.

Singtel released a statement on Thursday revealing that it was running Accellion's legacy file sharing system FTA to share information internally and with external stakeholders.

Cyber-criminals appear to have exploited potentially multiple FTA vulnerabilities in attacks against various customers.

Although Singtel said its core operations "remain unaffected and sound," it admitted there may be an impact on customers.

"We are currently conducting an impact assessment with the utmost urgency to ascertain the nature and extent of data that has been potentially accessed. Customer information may have been compromised," it explained.

https://www.infosecurity-magazine.com/news/singtel-supply-chain-breach-traced

Click link above to read more

Click Unsubscribe to stop receiving the Digest.

****

For previous issues of Security News Digest, visit the current month archive page at:

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