Security News Digest
Information Security Branch

OCIO Office of the Chief Information Officer

January 28th, 2020

Try our January Quiz - Resolutions

Save the date - February 5th to 7th is the Privacy and Security Conference

This week's stories:

- **Mastercard Commits $510 million for new global cybersecurity centre in Vancouver**
- **Ontario construction firm victim of ransomware attack**
- **Rogers' internal passwords and source code found open on GitHub**
- **Buchbinder Car Renter Exposes Info of Over 3 Million Customers**
- **NFL Twitter Accounts Hacked One Week Before Super Bowl**
- **Projects funded for autonomous vehicle cyber security**
- **The Jeff Bezos phone hack proves anyone can fall victim to cybersecurity attacks. But here's what security experts say you can do to reduce the risk.**
- **What Is Smishing, and How Do You Protect Yourself?**
- **Fake Smart Factory Honeypot Highlights New Attack Threats**
- **City of Potsdam Servers Offline Following Cyberattack**
- **Bipartisan Coalition Bill Introduced to Reform NSA Surveillance**
- **Microsoft Exposes 250M Customer Support Records on Leaky Servers**
- **Mozilla cleans house, bans and removes 197 malicious Firefox add-ons**

Mastercard Commits $510 million for new global cybersecurity centre in Vancouver

https://betakit.com/mastercard-commits-510-million-for-new-global-cybersecurity-centre-in-vancouver/

In an announcement at the fiftieth annual World Economic Forum currently being held in Davos, Switzerland, Minister Navdeep Bains and Ajay Banga, CEO of Mastercard, revealed today that Mastercard will open its latest global technology centre in Vancouver.

Mastercard is investing $510 million to build out the centre, intended to be an innovation hub for digital and cyber security, artificial intelligence (AI), and the Internet of Things (IoT). Called the Intelligence and Cyber Centre, the space is Mastercard's sixth global technology centre and its first in Canada.

Click link above to read more

Ontario construction firm victim of ransomware attack

https://www.itworldcanada.com/article/ontario-construction-firm-victim-of-ransomware-attack/426487

A multi-million dollar Ontario construction firm that has worked on major federal and provincial projects including facilities for national defence and police stations has been hit by a ransomware attack.

According to CBC News, Bird Construction of Mississauga, Ont., acknowledged that it was recently victimized, but didn't give any details.

Click link above to read more

Rogers' internal passwords and source code found open on GitHub

https://www.itworldcanada.com/article/rogers-internal-passwords-and-source-code-found-open-on-github/426429

Sensitive data of another major Canadian firm has been found sitting open on the GitHub developers platform.

Security researcher Jason Coulls said he recently discovered two open accounts with application source code, internal user names and passwords, and private keys for Rogers Communications. No customer data was found.

Click link above to read more

Buchbinder Car Renter Exposes Info of Over 3 Million Customers

https://www.bleepingcomputer.com/news/security/buchbinder-car-renter-exposes-info-of-over-3-million-customers/

German car rental company Buchbinder exposed the personal information of over 3.1 million customers including federal ministry employees, diplomats, and celebrities, all of it stored within a ten terabytes MSSQL backup database left unsecured on the Internet.

The German company runs a worldwide network of over 5000 car rental stations directed by partners and franchise holders, with clients from more than 100 countries.

Buchbinder is currently investigating the security breach according to a notification displayed on the company's website.

Click link above to read more

NFL Twitter Accounts Hacked One Week Before Super Bowl

https://www.infosecurity-magazine.com/news/nfl-twitter-accounts-hacked/

The Twitter accounts of America's National Football League (NFL) and 15 of its teams have been hacked just one week before the biggest football game of the 2019–2020 season.

The first team to be compromised was the Chicago Bears, whose account @ChicagoBears was hacked at 8:40 a.m. on Sunday morning.

Followers were shown an image of a man with a full, dark beard who was wearing the traditional Arabic head gear of a keffiyeh and an agal together. Along with the photo, hackers posted the caption: "Welcome to our new owner @Turki_alalshikh #ProBowl #Bears100 #ChicagoBears."

Click link above to read more

Projects funded for autonomous vehicle cyber security

https://www.theengineer.co.uk/cyber-security-autonomous-vehicles/

The £1.2m award has been made by Zenzic, an organization dedicated to making the UK a world leader in connected and autonomous mobility.

According to Zenzic, the Cyber Securities Feasibility studies competition is part-funded by the Centre for Connected and Autonomous Vehicles (CCAV) and delivered in partnership with Innovate UK.

In a statement, Richard Porter, Zenzic's technology and innovation director said: "With the advent of self-driving vehicles, the complexity of cyber defences will increase as thousands of vehicles, pieces of road-side infrastructure and connecting systems need to share data securely. This is an opportunity for the UK to build on the decades of experience we already have and once again set the standards for the rest of the world to follow."

Click link above to read more

The Jeff Bezos phone hack proves anyone can fall victim to cybersecurity attacks. But here's what security experts say you can do to reduce the risk.

https://www.businessinsider.com/jeff-bezos-phone-hacked-whatsapp-security-experts-2020-1

Saudi Crown Prince Mohammed bin Salman reportedly hacked Amazon CEO Jeff Bezos' phone in 2018, an infiltration that is said to have resulted in large amounts of data being covertly stolen from the tech executive's phone over the course of months.

The incident was revealed in a forensic investigation conducted by FTI Consulting that was first reported by The Guardian earlier this week. The United Nations has since called on the United States and other relevant authorities to conduct an investigation. The Saudi government denied the allegations against it and called them "absurd."

Click link above to read more

What Is Smishing, and How Do You Protect Yourself?

https://www.howtogeek.com/526115/what-is-smishing-and-how-do-you-protect-yourself/

By now, almost everyone has encountered phishing scams that arrive via spam emails. For example, someone might claim to be from your bank and request you provide account information, social security numbers, or credit card details.

Smishing is just the SMS version of phishing scams. Instead of a scammy email, you get a scammy text message on your smartphone. "SMS" stands for "short message service" and is the technical term for the text messages you receive on your phone.

Click link above to read more

Fake Smart Factory Honeypot Highlights New Attack Threats

https://threatpost.com/fake-smart-factory-honeypot-highlights-new-attack-threats/152170/

A honeypot set up to observe the current security landscape in smart manufacturing systems observed numerous threats—including cryptomining malware and ransomware—in just a few months, highlighting the new threats that industrial control systems (ICS) face with increased exposure to the internet.

While in the past ICS networks were traditionally proprietary and closed systems, the advent of the Internet of Things (IoT) has created manufacturing systems that have exposed devices and network ports to the internet. This also makes these systems vulnerable to more threats from bad actors – which could have dire implications when it comes to manufacturing plants or critical infrastructure.

Click link above to read more

City of Potsdam Servers Offline Following Cyberattack

https://www.bleepingcomputer.com/news/security/city-of-potsdam-servers-offline-following-cyberattack/

The City of Potsdam severed the administration servers' Internet connection following a cyberattack that took place earlier this week. Emergency services including the city's fire department fully operational and payments are not affected.

Potsdam is the largest city and the capital of the German federal state of Brandenburg, bordering the German capital, Berlin.

The systems of the Brandenburg capital are still offline after the unauthorized access to the Potsdam administration's servers was noticed on Tuesday and their Internet connection was shut down on Wednesday evening to prevent data exfiltration.

Click link above to read more

Bipartisan Coalition Bill Introduced to Reform NSA Surveillance

https://www.bleepingcomputer.com/news/security/bipartisan-coalition-bill-introduced-to-reform-nsa-surveillance/

A bipartisan coalition of U.S. lawmakers introduced a new bill that wants to protect Americans from warrantless government surveillance such as the one run by the National Security Agency (NSA).

The Safeguarding Americans' Private Records Act was introduced today by Senators Wyden and Daines in the upper chamber, the Senate, while Representatives Lofgren, Davidson and Jayapal introduced it in the lower chamber, the US House of Representatives.

This bill arrives before the March 15 expiration of Section 215 of the PATRIOT Act, used by the National Security Agency "to create a secret mass surveillance program that swept up millions of Americans' phone calls."

Click link above to read more

Microsoft Exposes 250M Customer Support Records on Leaky Servers

https://www.bleepingcomputer.com/news/security/microsoft-exposes-250m-customer-support-records-on-leaky-servers/

Microsoft disclosed a security breach caused by a misconfigured internal customer support database that led to the accidental exposure of roughly 250 million customer support and service records, some of them containing personally identifiable information.

"Our investigation has determined that a change made to the database's network security group on December 5, 2019 contained misconfigured security rules that enabled exposure of the data," Microsoft said in a blog post published today.

Click link above to read more

Mozilla cleans house, bans and removes 197 malicious Firefox add-ons

https://www.itworldcanada.com/article/mozilla-cleans-house-bans-and-removes-197-malicious-firefox-add-ons/426535

It seems that Mozilla's quest for protecting privacy in its products has intensified.

The company has recently banned 197 Firefox add-ons that its add-on review team caught gathering user data illegally, executing malicious code, or using obfuscation.

Mozilla has banned and removed the identified add-ons from Mozilla Add-on (AMO) portal in order to make sure any new installs are prevented. In addition, the company has also disabled these add-ons, if already installed, from the users' browsers.

Click link above to read more

---

their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity of each article and to apply their own judgment when using or referring to this information. The ISB is not responsible for the manner in which the information presented is used or interpreted by its recipients.

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:

Information Security Awareness Team - Information Security Branch
Office of the Chief Information Officer,
Ministry of Citizens' Services
4000 Seymour Place, Victoria, BC V8X 4S8

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