December 31st, 2019

Try our December quiz – Shopping Safety

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

This week's stories:

- **LifeLabs facing proposed class action over data breach affecting up to 15M clients**
- **Ontario's healthcare shakeup attracting cyberattacks, says security expert**
- **A decade of hacking: The most notable cyber-security events of the 2010s**
- **Christmas malware uses "Support Greta Thunberg" as a lure**
- **Christmas Is Here Again! - Stay "Cyber Safe" As You Enjoy**
- **Cybersecurity in 2020: Eight frightening predictions**
- **Criminals Pull Hard Before Xmas, Attack U.S. Health Industry**
- **Microsoft Takes North Korean Hacking Group Thallium to Court**
- **Ransomware Hits Maastricht University, All Systems Taken Down**
- **Employee error to blame for massive data leak, Wyze says**

LifeLabs facing proposed class action over data breach affecting up to 15M clients

https://www.canadiansecuritymag.com/lifelabs-facing-proposed-class-action-over-data-breach-affecting-up-to-15m-clients/

TORONTO — A proposed class action lawsuit has been filed against medical services company LifeLabs over a data breach that allowed hackers to access the personal information of up to 15 million customers.

In an unproven statement of claim filed in Ontario Superior Court on Dec. 27, lawyers Peter Waldmann and Andrew Stein accuse LifeLabs of negligence, breach of contract and violating their customers' confidence as well as privacy and consumer protection laws.

Click link above to read more

Ontario's healthcare shakeup attracting cyberattacks, says security expert

https://www.itworldcanada.com/article/ontarios-healthcare-shakeup-attracting-cyberattacks-says-security-expert/

The Ontario government has described its new model for healthcare as the biggest health system reform in 50 years, but according to a security expert, it's leading to a spike in cyberattacks.

The province's ongoing efforts to merge its health agencies and create local care co-ordination organizations called Ontario Health Teams are absent of a proper security framework, indicated Raheel Qureshi, the co-founder, and partner of iSecurity.

"What's happening as a result of [the mergers] is hospitals are opening up their network to start to collaborate, but they aren't talking security yet," he told IT World Canada. "If I compromise one hospital, guess what? I can potentially get into 10 other hospitals and I can hold each one for ransom."

Click link above to read more

A decade of hacking: The most notable cyber-security events of the 2010s

https://www.zdnet.com/article/a-decade-of-hacking-the-most-notable-cyber-security-events-of-the-2010s/

The 2010s decade is drawing to a close and ZDNet is looking back at the most important cyber-security events that have taken place during the past ten years.

Over the past decade, we've seen it all. We've had monstrous data breaches, years of prolific hacktivism, plenty of nation-state cyber-espionage operations, almost non-stop financially-motivated cybercrime, and destructive malware that has rendered systems unusable.

Click link above to read more

Christmas malware uses "Support Greta Thunberg" as a lure

https://nakedsecurity.sophos.com/2019/12/27/christmas-malware-uses-support-greta-thunberg-as-a-lure/

SophosLabs has a seen a variety of Christmas-time spam campaigns that shamlessly hitch a ride on the coat-tails of climate activist Greta Thunberg.

The malware-spreading spams arrive with subject lines such as…

```
Please help save the planet

Greta

Friends help

Support Greta Thunberg - Time Person of the Year 2019

Greta Thunberg

the biggest demonstration

Demonstration 2019
```

Click link above to read more

Christmas Is Here Again! - Stay "Cyber Safe" As You Enjoy

https://www.modernghana.com/news/975848/christmas-is-here-again-stay-cyber-safe-as.html

Christmas period is unarguably the busiest period as compared to all other festive seasons within the year. As such, online activities and electronic transactions tend to increase. People will be sending and receiving gifts mostly through electronic means (Mobile money transfers, foreign remittances, credit & debit cards transactions, internet payments, ATM transactions, etc.).

More people will also be working from home, sending and receiving emails, using the Internet and accessing online web portals.

The season also presents a good opportunity for cyber-criminals to exploit. While people prepare for the festivities, cyber-criminals also look for opportunities to scam shoppers with various tricks.

Click link above to read more

Cybersecurity in 2020: Eight frightening predictions

https://www.techrepublic.com/article/the-state-of-security-in-2020/

The coming year looks promising on many levels; however, there could also be an inordinate rise of security breaches, attacks, and incidents. What will make 2020 such a banner year is that hackers will start turning technology against the companies that deploy it.

Confused? Let's dive in so I can explain what I believe will make 2020 reset the bar for security attacks.

Click link above to read more

Criminals Pull Hard Before Xmas, Attack U.S. Health Industry

https://www.bleepingcomputer.com/news/security/criminals-pull-hard-before-xmas-attack-us-health-industry/

Attackers are taking no breaks and actually pull harder before holidays, as shown by a San Antonio mental health services provider and a New Mexico hospital impacted by malware attacks according to reports and disclosures published before Christmas.

San Antonio's The Center for Health Care Services (CHSC) shut down computing systems for all its clinics in response to a larger-scale cyber-attack that took place last week.

Roosevelt General Hospital (RGH), the other healthcare organization affected, disclosed that it discovered malware on one of its digital imaging servers containing patient info, on November 14.

Click link above to read more

Microsoft Takes North Korean Hacking Group Thallium to Court

https://www.bleepingcomputer.com/news/security/microsoft-takes-north-korean-hacking-group-thallium-to-court/

Microsoft sued a cyber-espionage group with North Korean links tracked as Thallium for breaking into its customers' accounts and networks via spear-phishing attacks with the end goal of stealing sensitive information, as shown by a complaint unsealed on December 27.

"To manage and direct Thallium, Defendants have established and operate a network of websites, domains, and computers on the Internet, which they use to target their victims, compromise their online accounts, infect their computing devices, compromise the security of their networks, and steal sensitive information from them," Microsoft's complaint says.

Click link above to read more

Ransomware Hits Maastricht University, All Systems Taken Down

https://www.bleepingcomputer.com/news/security/ransomware-hits-maastricht-university-all-systems-taken-down/

Maastricht University (UM) announced that almost all of its Windows systems have been encrypted by ransomware following a cyber-attack that took place on Monday, December 23.

UM is a university from the Netherlands with over 18,000 students, 4,400 employees, and 70,000 alumni, UM being placed in the top 500 universities in the world by five ranking tables in the last two years.

"Maastricht University (UM) has been hit by a serious cyber-attack," the university announced on Christmas Eve, December 24.

Click link above to read more

Employee error to blame for massive data leak, Wyze says

https://arstechnica.com/tech-policy/2019/12/surveillance-camera-company-wyze-confirms-leak-of-user-data/

Loads of folks found brand-new Wyze surveillance cameras under their trees or in their stockings this Christmas. And on Boxing Day, the company itself unwrapped a whole new world of trouble for everyone who uses its products, confirming a data leak that may have exposed personal data for millions of users over the course of a few weeks.

Wyze first found out about the problem on the morning of December 26, company cofounder Dongsheng Song said in a corporate blog post. The company's investigation confirmed that user data was "not properly secured" and was exposed from December 4 onward.

Click link above to read more


Security News Digest
Information Security Branch
BRITISH COLUMBIA
OCIO
Office of the Chief Information Officer