January 4, 2022

Challenge yourself with our NEW Cyber Security Resolutions quiz!

This past week's stories:

- 2021: 'A crazy mess': Cybersecurity year in review and look ahead
- Saskatchewan Liquor and Gaming Authority joins growing list of organizations facing cyberattacks
- Montreal tourism agency confirms cyber attack
- 5 cybersecurity trends to watch in 2022
- Stay vigilant and aware, cyber attacks will continue to increase in 2022
- Breaking the habit: Top 10 bad cybersecurity habits to shed in 2022
- Protecting your data from a unique threat: Misinformation
- Opportunity not fear: Reframing cybersecurity to build a safer net for all
- Cyber world is starting 2022 in crisis mode with the log4j bug
- Florida's Broward Health confirms October 2021 breach
- Google disrupts major malware distribution network Glupteba
- Google launches hacker crack down as it snaps up Israeli cybersecurity firm Siemplify for £371m

---

2021: 'A crazy mess': Cybersecurity year in review and a look ahead

When Brett Callow, B.C.-based threat analyst for Emsisoft was asked to describe 2021, he reduced it to three words: "A crazy mess."

The mess started in January, with CISOs scrambling for evidence their networks had been compromised by the SolarWinds Orion hack, and went on from there, with CISOs learning that other platforms in the supply chain, such as Kaseya and Accellion FTA had been compromised, rushing to patch on-premises Microsoft Exchange servers in the wake of the Hafnium compromise, realizing the vulnerability of critical infrastructure after the (thankfully interrupted) attack on a Florida water treatment plant and the ransomware attack on the U.S. Colonial Pipeline. It ended with them scrambling for evidence their networks had been compromised by the Log4j2 bugs.

https://www.itworldcanada.com/article/2021-a-crazy-mess-cybersecurity-year-in-review-and-a-look-ahead/469389

Click above link to read more.

Back to top

Saskatchewan Liquor and Gaming Authority joins growing list of organizations facing cyberattacks

The Saskatchewan Liquor and Gaming Authority is investigating a cyberattack, after it was hit on Christmas Day.

The Crown corporation, which is headquartered in Regina, operates about 35 liquor stores in 24 communities, is responsible for regulating alcohol and cannabis and also operates and regulates many forms of gaming throughout the province.

https://www.cbc.ca/news/canada/saskatchewan/slga-cyber-security-breach-1.6300182

Click above link to read more.

Back to top

Montreal tourism agency confirms cyberattack

Montreal's tourism agency has acknowledged it was hit by a cyber attack early last month, one of a number of recent Canadian and American victim organizations claimed by the Karakurt hacking group.

"Tourisme Montréal can confirm that it became aware of a cybersecurity incident that we experienced on December 7th," Francis Bouchard, the agency's manager of corporate communications and public affairs, said in a statement on Tuesday.

https://www.itworldcanada.com/article/montreal-tourism-agency-confirms-cyber-attack/469873

Click above link to read more.

Back to top

---

5 cybersecurity trends to watch in 2022

No one could have predicted the sheer chaos the cybersecurity industry would experience over the course of 2021. Record-annihilating numbers of ransomware attacks, SolarWinds' supply-chain havoc and most recently, the discovery of Log4j by…Minecraft gamers. All of it would have sounded too wild for real life a short year ago.

Yet here we are.

https://threatpost.com/5-cybersecurity-trends-2022/177273/

Click above link to read more.

Back to top

Stay vigilant and aware, cyber attacks will continue to increase in 2022

Protecting yourself from new online threats such as Log4J is now more important than ever, warns cybersecurity and digital forensic expert Ricoh Danielson.

Log4J allows threat actors to access your computer without you knowing it.

This online vulnerability is hidden in standard Microsoft code. Chinese and Korean scammers could possibly use it to transfer your entire identity including passwords, financial information, nationality, and other biometric information.

https://finance.yahoo.com/news/stay-vigilant-aware-cyber-attacks-134000148.html

Click above link to read more.

Back to top

Breaking the habit: Top 10 bad cybersecurity habits to shed in 2022

The new year is a new opportunity to rewire your digital life. An increasingly important part of this is cybersecurity. In fact, 2021 is already shaping up to have been one of the most prolific years yet for cybercriminals. Almost 19 billion records were exposed in the first half of the year alone.

Better security should mean you're more insulated from the risk of identity fraud and financial loss. The cost of these scams reached a record $56bn in 2020, with most of this coming online. Although the organizations you interact with have a duty, and often a legal responsibility, to keep your data protected, it's important to do your bit.

https://www.welivesecurity.com/2022/01/03/breaking-habit-top-10-bad-cybersecurity-habits-shed-2022/

Click above link to read more.

Back to top

Protecting your data from a unique threat: Misinformation

It's the target for attackers. It drives unique insights and innovation. Data is the most valuable asset your organization has. Now, more than ever before, your company's information faces a unique threat — one for which many cybersecurity teams aren't prepared — misinformation.

The value of data isn't lost on most cybersecurity leaders, but data is simply information. And what if that information is actually misinformation? Or disinformation? How can your cybersecurity program determine what's real and what's not real?

https://securityintelligence.com/articles/protecting-data-from-misinformation-cybersecurity/

Click above link to read more.

Back to top

Opportunity not fear: Reframing cybersecurity to build a safer net for all

Throughout 2021, global news seemed to ricochet between the rapid spread of new iterations of COVID-19 and cyber criminality — both becoming increasingly creative and disruptive as they mutate in a battle for survival; both interlinked as cybercriminals profit from rapid digitalization forced by COVID-19 lockdowns. In a recent interview, a prominent cybersecurity executive pointed out that alongside birth, death and taxes, the only other guarantee in our current lives is the exponential growth of digital threats.

https://techcrunch.com/2022/01/04/2252633/

Click above link to read more.

Back to top

Cyber world is starting 2022 in crisis mode with the log4j bug

Welcome back to The Cybersecurity 2022! My household managed to see family in Iowa and North Carolina over the holiday break and return to negative coronavirus tests. I wish everyone was so lucky.

The cybersecurity world is starting off 2022 in crisis mode.

The newest culprit is the log4j software bug, which Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly called “the most serious vulnerability I have seen in my decades-long career.” It forced many cybersecurity pros to work through the holidays to protect computer systems at Big Tech firms, large and small companies and government agencies.

https://www.washingtonpost.com/politics/2022/01/03/cyber-world-is-starting-2022-crisis-mode-with-log4j-bug/

Click above link to read more.

Back to top

Florida's Broward Health confirms October 2021 breach

Florida's Broward Health hospital system has notified employees and patients of a data breach that occurred on Oct. 15 and compromised a wide range of personal and medical information.

An attacker gained entry to the Broward Health network via the office of a third-party medical provider that was allowed access to the system to provide healthcare services, officials confirm in a disclosure of the incident. Broward Health detected the attack on Oct. 19 and contained the incident, alerted the FBI and Department of Justice (DoJ), required employees to reset their passwords, and hired an external security firm as part of its investigation, officials wrote.

https://www.darkreading.com/attacks-breaches/florida-s-broward-health-confirms-october-2021-breach

Click above link to read more.

Back to top

Google disrupts major malware distribution network Glupteba

Working with several internet infrastructure and hosting providers, including Cloudflare, Google disrupted the operation of an aggressive Windows botnet known as Glupteba that was being distributed through fake ads. It also served itself as a distribution network for additional malware. The company also filed a lawsuit against two individuals believed to be based in Russia and who play a central role in operating the botnet.

Google's action targeted key command-and-control infrastructure such as servers and domain names used by Glupteba, as well as many rogue accounts on Google's services that were being used to distribute it. While this is a severe blow to the botnet, whose estimated size is over 2 million computers, it's unlikely to be its demise because Glupteba has a backup command-and-control (C&C) mechanism that relies on the Bitcoin blockchain. This provides it with resilience against takedown attempts.

https://www.csoonline.com/article/3643706/google-disrupts-major-malware-distribution-network-glupteba.html

Click above link to read more.

Back to top

Google launches hacker crack down as it snaps up Israeli cybersecurity firm Siemplify for £371m

Google, also known as Alphabet, has acquired Israeli cybersecurity startup Siemplify for an estimated $500m (£371m), as the giant gears up for the rise in cyber attacks and data breaches.

Siemplify has raised $58m (£43m) over four rounds to date, with Israeli VC G20 Ventures the company's largest shareholder.

https://www.cityam.com/google-snaps-up-israeli-cybersecurity-firm-siemplify-for-371m-amid-hacker-crack-down/

Click above link to read more.

Back to top