March 1, 2022

Challenge yourself with our Fraud Prevention quiz!

This past week's stories:

- Russia cyber warfare is a problem for everyone, experts warn
- Canadian companies at risk from Russia cyberattacks in retaliation from sanctions
- Halifax company that wants to assemble fighter jets comes under cyber attack

How can you verify information coming out of Russia or Ukraine? An expert's general guide on how to identify fake news

Moscow Exchange downed by cyber attack

NHS tells hospitals to shore-up cyber security amid fears Russian hackers may carry out WannaCry-style attack in retaliation for Ukraine invasion sanctions - as it's revealed 11 trusts get energy from Kremlin-backed firm Gazprom

Isle of Man kettle-parts firm hit by cyber attack

Chinese cybersecurity company Doxes Apparent NSA Hacking Operation

Toyota to close Japanese factories after suspected cyber-attack

Scenic Group announces cyber security breach

How to manage imposter syndrome in cyber security

Strengthening cyber security for today's remote workforce

Less than half of organizations say they have high confidence in the security of their Linux servers, according to new research from Synaptic Security

---

Russia cyber warfare is a problem for everyone, experts warn

Canada is reviewing its cyber defences to make sure it's secured against potential cyberattacks from an increasingly aggressive Russia. Experts say you should do the same at home.

While cyberattacks are already pummelling Ukraine, they could affect the average Canadian in a number of ways, too. They could hit your pocketbook, permanently wipe important files or sentimental photos from your electronics. In severe instances, they could disrupt critical infrastructure we rely on.

https://globalnews.ca/news/8650575/russia-ukraine-canada-cyberattack-cyberspace-cybersecurity/

Click above link to read more.

Back to top

Canadian companies at risk from Russia cyberattacks in retaliation from sanctions

Canadian businesses are at risk of being targeted for online attacks if Russia chooses to retaliate against government sanctions, a cybersecurity expert said Friday.

Karim Hijazi, founder and CEO of Texas-based cyberintelligence firm Prevailion, said that Canadian companies could be victims of bad actors trying to compromise critical infrastructure and government entities.

https://www.cp24.com/news/canadian-companies-at-risk-from-russia-cyberattacks-in-retaliation-from-sanctions-1.5797191

Click above link to read more.

Back to top

Halifax company that wants to assemble fighter jets comes under attack

The Nova Scotia company vying to replace Canada's aging fleet of fighter jets came under an attack of a different nature recently, with a computer virus infiltrating IMP Group's servers through an email.

The company is still scanning its servers, which have been slowed considerably by the effort in the wake of the cyber-attack that introduced a virus into the system.

https://www.saltwire.com/atlantic-canada/news/halifax-company-that-wants-to-assemble-fighter-jets-comes-under-cyber-attack-100699645/

Click above link to read more.

Back to top

How can you verify information coming out of Russia or Ukraine? An expert's general guide on how to identify fake news

We've all seen COVID-19 misinformation and disinformation online. Now, with many videos, images and news coming out of Ukraine, among other war-torn countries, it may be hard to identify what is real and what isn't.

To help prevent the spread of fake news, it's important to verify sources and content posted on websites or social media. But how can you do that?

https://www.thestar.com/news/gta/2022/02/28/how-can-you-verify-information-coming-out-of-russia-or-ukraine-an-experts-general-guide-on-how-to-identify-fake-news.html

Click above link to read more.

Back to top

Moscow Exchange downed by cyber attack

The website for the Moscow Stock Exchange was offline and inaccessible on Monday.

A crowdsourced community of hackers endorsed by Kyiv officials has claimed responsibility for the outage. The Ukraine IT Army posted a message on Telegram that it had taken just five minutes to render the site inaccessible.

A spokesperson for global internet connectivity tracking company Netblocks told Forbes: “We can confirm the Moscow Exchange website is down, but we don’t have visibility into the incident’s root cause or the extent of the disruption.”

https://www.infosecurity-magazine.com/news/moscow-exchange-cyber-attack/

Click above link to read more.

Back to top

NHS tells hospitals to shore-up cyber security amid fears Russian hackers may carry out WannaCry-style attack in retaliation for Ukraine invasion sanctions - as it's revealed 11 trusts get energy from Kremlin-backed firm Gazprom

NHS trusts have been told to firm up their cybersecurity amid fears of a Russian attack in retaliation to Western interference in the war in Ukraine.

Health chiefs have written to hospitals telling them to make it their 'focus' to keep their systems secure and make sure backups are in place.

There have been widespread concerns about the technological resilience of the NHS which only last year stopped using fax machines.

https://www.dailymail.co.uk/news/article-10565149/NHS-tells-hospitals-shore-cyber-security-amid-fears-Russian-hack.html

Click above link to read more.

Back to top

Isle of Man kettle-parts firm hit by cyber attack

An Isle of Man firm which makes kettle safety controls has said it has been hit by a cyber attack "of Russian origin".

Strix Group said its servers on the island and the UK were affected but systems were now "restored".

There has been "no impact on customer orders or sales", the company told the London Stock Exchange.

https://www.bbc.com/news/world-europe-isle-of-man-60555839

Click above link to read more.

Back to top

Chinese cybersecurity company doxes apparent NSA hacking operation

A Chinese cybersecurity company accused the NSA of being behind a hacking tool used for ten years in a report published on Wednesday.

The report from Pangu Lab delves into malware that its researchers first encountered in 2013 during an investigation into a hack against “a key domestic department.” At the time, the researchers couldn’t figure out who was behind the hack, but then, thanks to leaked NSA data about the hacking group Equation Group—widely believed to be the NSA—released by the mysterious group Shadow Brokers and by the German magazine Der Spiegel, they connected the dots and realized it was made by the NSA, according to the report.

https://www.vice.com/en/article/v7dxg3/chinese-cybersecurity-company-doxes-apparent-nsa-hacking-operation

Click above link to read more.

Back to top

Toyota to close Japanese factories after suspected cyber-attack

Toyota will shut down all 14 of its factories in Japan on Tuesday after a possible cyber-attack.

News site Nikkei, which first reported the shutdown, said supplier Kojima Industries Corporation suspected it had been hit by a cyber-attack, causing a halt in production.
Japanese factories account for about a third of Toyota's production.

https://www.bbc.com/news/technology-60521983

Click above link to read more.

Back to top

Scenic Group announces cyber security breach

Officials from Scenic Group announced on Monday the company experienced a cyber security incident involving unauthorized access to IT systems.

Scenic Group Chief Operating Officer Rob Voss said in a statement the company’s teams had isolated the IT systems to minimize any further impact and launched a formal investigation into the breach. Officials hired external cyber security forensic experts to resolve the situation and bring systems back online.

https://www.travelpulse.com/news/impacting-travel/scenic-group-announces-cyber-security-breach.html

Click above link to read more.

Back to top

How to manage imposter syndrome in cyber security

Cybersecurity is often viewed as a highly technical industry. This perception is largely accurate; however, a lack of technical knowledge shouldn't prevent someone from exploring a cybersecurity career.

"If someone has a lot of intangible qualities about them, they'll likely be a good fit for a role in security," said Alyssa Miller, author of Cyber Security Career Guide. "Once they're in the role, managers can bring them in and help them develop on the technical side because they have the other pieces -- like natural curiosity or problem-solving or empathy."

https://www.techtarget.com/searchsecurity/feature/How-to-manage-imposter-syndrome-in-cybersecurity

Click above link to read more.

Back to top

Strengthening cyber security for today's remote workforce

Even as businesses reopen after a historic pandemic, it is clear that the workplace has changed forever. Organizations that might have been slow to adopt remote networking have widely deployed innovative solutions, and most of them like what they see. According to Gartner, 82% of business leaders surveyed plan to maintain at least a partial work-from-home structure even after the pandemic has fully passed.

Employee expectations have evolved as well. In a recent McKinsey survey, more than 50% of employees indicated they would like to work from home for three or more days every week. However, just as the workplace has changed, new cybersecurity issues have emerged. Today's cybercriminals are refining their threats to take advantage of the public's concerns about Covid-19. According to research by Forcepoint, cyberattacks sent 1.5 million malicious emails per day related to the pandemic over a three-month period. In a world of increasingly hybrid workplace environments, it's important for organizations to step back and take a closer look at the security processes and infrastructure that support their remote workforces.

https://www.forbes.com/sites/forbestechcouncil/2022/02/28/strengthening-cybersecurity-for-todays-remote-workforce/?sh=7f7b9f57400e

Click above link to read more.

Back to top

Less than half of organizations say they have high confidence in the security of their Linux servers, according to new research from Synaptic Security

Following the exposure of massive cybersecurity vulnerabilities over the past two years, three out of four organizations have experienced a cybersecurity attack, one-third of which happened within the last six months, according to new research from Synaptic Security. Further, most organizations believe they are *not* fully prepared for ransomware and other security threats. The result: cybersecurity is a top business priority for the next 12-24 months, even more important than new customer acquisition and operational efficiency. In fact, 75 percent of those surveyed say the challenges of managing cyber threats, especially within Linux environments, will only increase in 2022 and beyond.

https://www.businesswire.com/news/home/20220228005328/en/Less-Than-Half-of-Organizations-Say-They-Have-High-Confidence-in-the-Security-of-Their-Linux-Servers-According-to-New-Research-from-Synaptic-Security

Click above link to read more.

Back to top

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