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

January 16, 2024

Challenge yourself with our Quishing Quiz!

Cybersecurity Issue of the Week: **Ransomware**

✪ Check out our **Ransomware Infosheet** to learn more.

Wonder what you can do to protect yourself from ransomware?

All Users	Technical Users	Business Owners
It's never a bad idea to be overly cautious, so if you find an ad that appeals to you on a third-party website, search it up on Google and go directly to the seller's site, instead of clicking on the ad on the webpage.	If you find the ad interesting, Google it instead and go to the seller's site directly. It's best to do this on your personal computer instead of your work one. If somehow your work computer becomes compromised, it could infect other work computers in your office as part of a chain attack.	Consider implementing enterprise level anti-virus software onto your organization's devices.

This past week's stories:

🍁 **'Sent from my iPhone': Public warned of extra deceptive gift card scam**
🍁 **IT World Canada strikes partnership with Canadian Cybersecurity Network**
✪ 🍁 **Data from U of T students threatened by MOVEit ransomware attack**
🍁 **Canadian Centre for Cyber Security and SecurityScorecard establish partnership to strengthen cyber resilience and secure critical infrastructure**
98% of basic cybersecurity hygiene could prevent a cyberattack for most NGOs
Living-off-Trusted-Sites (LOTS) – APT hackers abusing GitHub to deliver malware payload
Opera MyFlaw bug could let hackers run ANY file on your Mac or Windows
Australia's strategy to become a global cyber leader by 2030

Cosmetics retailer Lush dealing with mystery cyber incident
Trellix announces advanced ransomware detection and response solution
Hackers impersonating as security researcher to aid ransomware victims
Female cyber pros group targeted in phishing scam
29-year-old Ukrainian cryptojacking kingpin arrested for exploiting cloud services
Cybersecurity is on the frontline of our AI future. Here's why

---

‘Sent from my iPhone’: Public warned of extra deceptive gift card scam

The Better Business Bureau (BBB) is warning the public about a new gift card scam that’s so well-crafted, it almost fooled the non-profit’s own staff.

https://globalnews.ca/news/10227871/better-business-bureau-gift-card-scam/#:~:text=The%20BBB%20is%20advising%20anyone,on%20payment%20with%20gift%20cards

Click above link to read more.

Back to top

IT World Canada strikes partnership with Canadian Cybersecurity Network

Two of Canada’s biggest cybersecurity news and events providers have struck a partnership to better serve infosec pros.

https://financialpost.com/technology/it-world-canada-strikes-partnership-with-canadian-cybersecurity-network

Click above link to read more.

Back to top

Data from U of T students threatened by MOVEit ransomware attack

U of T’s financial auditor Ernst & Young LLP (EY) contacted impacted students and staff members in November about a security breach that may have compromised sensitive personal information.

https://thevarsity.ca/2024/01/15/data-from-u-of-t-students-threatened-by-moveit-ransomware-attack/

Click above link to read more.

Back to top

Canadian Centre for Cyber Security and SecurityScorecard establish partnership to strengthen cyber resilience and secure critical infrastructure

SecurityScorecard, the global leader in security ratings, today announced a partnership with the Canadian Centre for Cyber Security (the Cyber Centre). SecurityScorecard is delivering security ratings with continuous real-time monitoring to manage cyber risk across Canada's critical infrastructure.

https://financialpost.com/pmn/business-wire-news-releases-pmn/canadian-centre-for-cyber-security-and-securityscorecard-establish-partnership-to-strengthen-cyber-resilience-and-secure-critical-infrastructure

Click above link to read more.

Back to top

98% of basic cybersecurity hygiene could prevent a cyberattack for most NGOs

According to a research, in 2023, 27% of nonprofits worldwide encountered a cyberattack. This sector appeals to cybercriminals for several reasons, the key being the high volumes of money generated from such attacks. For example, charities alone raised 12.7 billion in funds in the UK last year. Criminals seek out high-income charities with £500,000 or more in annual income in particular, and more than 56% of such charities have experienced a cyberattack.

https://www.dailyhostnews.com/98-of-basic-cybersecurity-hygiene-could-prevent-a-cyberattack-for-most-ngos

Click above link to read more.

Back to top

Living-off-Trusted-Sites (LOTS) – APT hackers abusing GitHub to deliver malware payload

Hackers use GitHub to access and manipulate source code repositories. GitHub hosts open-source projects, and unauthorized access allows hackers to inject malicious code, steal sensitive information, and exploit vulnerabilities in software development pipelines.

https://cybersecuritynews.com/living-off-trusted-sites-lots-apt-hackers/

Click above link to read more.

Back to top

Opera MyFlaw bug could let hackers run ANY file on your Mac or Windows

Cybersecurity researchers have disclosed a security flaw in the Opera web browser for Microsoft Windows and Apple macOS that could be exploited to execute any file on the underlying operating system.

https://thehackernews.com/2024/01/opera-myflaw-bug-could-let-hackers-run.html

Click above link to read more.

Back to top

Australia’s strategy to become a global cyber leader by 2030

Australia has set out a roadmap to realise its vision of becoming a world leader in cyber security by 2030.

The 2023–2030 Australian Cyber Security Strategy (13MB, PDF) sets out 6 cyber shields under which the Australian Government will seek to improve cyber security, manage cyber risks and better support citizens and businesses.

https://www.globalaustralia.gov.au/news-and-resources/news-items/australias-strategy-become-global-cyber-leader-2030

Click above link to read more.

Back to top

Cosmetics retailer Lush dealing with mystery cyber incident

Dorset-based cosmetics retailer Lush has fallen victim to a cyber security incident of a currently undisclosed nature, via a brief notice posted to its website on 11 January.

https://www.computerweekly.com/news/366566277/Cosmetics-retailer-Lush-dealing-with-mystery-cyber-incident

Click above link to read more.

Back to top

Trellix announces advanced ransomware detection and response solution

Trellix, the cybersecurity company delivering the future of extended detection and response (XDR), today announced Trellix XDR Platform for Ransomware Detection and Response (RDR), available immediately worldwide. Trellix XDR Platform for RDR provides visibility across an organization’s entire security ecosystem and delivers critical coverage for each stage of a ransomware campaign. The solution improves SOC efficiencies and strengthens operational resilience for customers, leveraging AI-guided capabilities to reduce the time to detect, investigate, and remediate ransomware threats.

https://www.businesswire.com/news/home/20240114676601/en/Trellix-Announces-Advanced-Ransomware-Detection-and-Response-Solution

Click above link to read more.

Back to top

Hackers impersonating as security researcher to aid ransomware victims

Hackers impersonate security researchers to exploit trust and credibility. By posing as legitimate figures in the cybersecurity community, they:

- Gain access to sensitive information
- Manipulate victims into compromising actions
- Enhance the success of their malicious activities while evading suspicion

https://cybersecuritynews.com/hackers-impersonating-as-security-researcher/

Click above link to read more.

Back to top

Female cyber pros group targeted in phishing scam

A threat actor is trying to con female cybersecurity pros into downloading malware.

The warning comes from the Canadian-based Women CyberSecurity Society (WCS2), which says someone is targeting members of the leadership team, members, and volunteers, trying to trick them into clicking on malicious links in text-based phishing messages, which is also called smishing.

https://www.itworldcanada.com/article/female-cyber-pros-group-targeted-in-phishing-scam/556096

Click above link to read more.

Back to top

29-year-old Ukrainian cryptojacking kingpin arrested for exploiting cloud services

A 29-year-old Ukrainian national has been arrested in connection with running a "sophisticated cryptojacking scheme," netting them over $2 million (€1.8 million) in illicit profits.

https://thehackernews.com/2024/01/29-year-old-ukrainian-cryptojacking.html

Click above link to read more.

Back to top

Cybersecurity is on the frontline of our AI future. Here's why

Three innovations have revolutionized the digital world in the last few decades: the internet, cloud and AI. Each technology took time for organizations to understand and adapt in the most productive and impactful way. To that end, AI is still in its infancy. But in just over a year, generative AI is on a trajectory from limited and mostly experimental applications to rapidly becoming an essential core technology.

https://www.weforum.org/agenda/2024/01/cybersecurity-ai-frontline-artificial-intelligence/

Click above link to read more.

Back to top

Click unsubscribe to stop receiving the Digest.

****
****

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase 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:

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

OCIOSecurity@gov.bc.ca

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.

Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO Office of the Chief Information Officer