December 17th, 2019

Try our December quiz – Shopping Safety

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

This week's stories:

- **Global News: City of Hamilton warns data breach may compromise residents' personal information.**
- **'Canadian eyes only' intelligence reports say Canadian leaders attacked in cyber campaigns**
- **49% of workers, when forced to update their password, reuse the same one with just a minor change**
- **Microsoft Found 44M Accounts Using Breached Passwords**
- **Microsoft Threat Protection Released in Public Preview.**
- **Security Flaws in Some Smartwatches Sold on Amazon May Let Strangers Track Kids**
- **New ransomware strain targets Western countries**
- **Amazon security: Patches fix multiple flaws exposing Blink cameras to hijacking.**
- **Microsoft details the most clever phishing techniques it saw in 2019.**
- **Visa Warns Of Rise In Gas Station POS Cyberattacks**
- **AI Firm Breaches Facial Recognition At Airports, Stores**

Global News: City of Hamilton warns data breach may compromise residents' personal information.

https://globalnews.ca/news/6285455/hamilton-data-breach/

The City of Hamilton is alerting residents of a "potential privacy breach" in which water-related billing data may have been accessed by third-party vendors.

In a release on Wednesday afternoon, the city said its water-related services, including meter reading, billing, payment, collections, and customer care services which are managed by Alectra Utilities, may have given access to customers' names, addresses, and tax assessment roll numbers.

Click link above to read more

'Canadian eyes only' intelligence reports say Canadian leaders attacked in cyber campaigns

https://globalnews.ca/news/6258755/intelligence-reports-canadian-leaders-attacked-cyber-campaigns/

Russia is one of the hostile foreign states that has targeted Canada in recent “cyber influence” campaigns, according to secret intelligence records obtained exclusively by Global News.

The records from Canada’s Communications Security Establishment (CSE) — labelled “Secret: Canadian Eyes Only” — say that due to their policies in eastern Europe, then-Minister of Foreign Affairs Chrystia Freeland and Minister of National Defence Harjit Sajjan are among the Canadian targets of “cyber influence activity to cause reputational damage.”

Click link above to read more

49% of workers, when forced to update their password, reuse the same one with just a minor change

https://www.grahamcluley.com/49-of-workers-when-forced-to-update-their-password-reuse-the-same-one-with-just-a-minor-change/

We all should know by now that credential stuffing and password reuse is a big problem.

Many computers users make the mistake of trusting the same password to protect their different online accounts, not realising that if one site gets hacked that may provide the key for hackers to break in elsewhere. Malicious attackers don’t have to do this by hand, they can use credential stuffing techniques to automatically throw databases of stolen usernames and passwords at a site to see which combination will grant them access.

Click link above to read more

Microsoft Found 44M Accounts Using Breached Passwords

https://www.pcmag.com/news/372398/microsoft-found-44m-accounts-using-breached-passwords

Microsoft has discovered 44 million user accounts are using usernames and passwords that have been leaked through security breaches.

As ZDNet reports, the vulnerable account logins were discovered when Microsoft's threat research team carried out a scan of all Microsoft accounts between January and March this year. The accounts were compared to a database of over three billion sets of leaked credentials and resulted in 44 million matches.

Click link above to read more

Microsoft Threat Protection Released in Public Preview.

https://www.bleepingcomputer.com/news/microsoft/microsoft-threat-protection-released-in-public-preview/

Microsoft says that the integrated Microsoft Threat Protection is now available in public preview, adding automated threat response to stop attacks in their tracks, as well as self-healing for compromised devices, user identities, and mailboxes.

Microsoft Threat Protection (MTP) is designed to consolidate a security team's incident response process by integrating key capabilities across Microsoft Defender Advanced Threat Protection (ATP), Office 365 ATP, Microsoft Cloud App Security, and Azure ATP.

Click link above to read more

Security Flaws in Some Smartwatches Sold on Amazon May Let Strangers Track Kids

https://ipv6.net/news/security-flaws-in-some-smartwatches-sold-on-amazon-may-let-strangers-track-kids/

Security researchers discovered vulnerabilities in cheap smartwatches for children that make it possible for strangers to override parental controls and track kids.

Rapid7 Inc., a cybersecurity firm based in Boston, purchased three smartwatches on Amazon.com, costing from $20 to $35, according to Deral Heiland, research lead for IoT technology. He said the models — GreaSmart Children's SmartWatch, Jsbaby Game Smart Watch and SmarTurtle Smart Watch for Kids — were picked randomly from dozens for sale on Amazon and marketed as appropriate for grade school-aged kids.

Click link above to read more

New ransomware strain targets Western countries

https://www.itworldcanada.com/article/new-ransomware-strain-targets-western-countries-says-report/425117

Infosec pros in North America and Europe are being warned of a new ransomware strain.

Researchers at Blackberry Cylance have dubbed this strain "Zeppelin," and said it has been targeting "carefully chosen" technology and healthcare firms since November.

This news comes as security vendor Emsisoft issued a report saying ransomware has hit crisis proportions in the U.S.

Zeppelin is part of a ransomware-as-a-service family known to some as Vega or VegaLocker. The two-share code and features, the researchers said in a blog post this week. However, Vega is distributed alongside other widespread financial malware as part of a malvertising operation aimed broadly at Russian-speaking computer users. Zeppelin is more targeted at potential victims, and it will quit if it infects machines that are based in Russia, Ukraine, Belorussia and Kazakhstan.

Click link above to read more

Amazon security: Patches fix multiple flaws exposing Blink cameras to hijacking.

https://www.zdnet.com/article/amazon-security-patches-fix-multiple-flaws-exposing-blink-cameras-to-hijacking/

Amazon has released updates to its Blink XT2 home security cameras after researchers discovered multiple flaws that could let nearby hackers hijack the cameras.

Researchers at Tenable Security reported several command-injection vulnerabilities to Amazon in August, which the company began rolling fixes out for in December. Users of Blink XT2 cameras should check that their firmware is version 2.13.11 or later, says Tenable.

Click link above to read more

Microsoft details the most clever phishing techniques it saw in 2019.

https://www.zdnet.com/article/microsoft-details-the-most-clever-phishing-techniques-it-saw-in-2019/

Earlier this month, Microsoft released a report on this year's malware and cyber-security trends. Among the few trends highlighted in the report was that phishing was one of the few attack vectors that saw a rise in activity over the past two years.

Microsoft said that phishing attempts grew from under 0.2% in January 2018 to around 0.6% in October 2019, where 0.6% represented the percentage of phishing emails detected out of the total volume of emails the company analyzed.

Click link above to read more

Visa Warns Of Rise In Gas Station POS Cyberattacks

https://www.pymnts.com/news/security-and-risk/2019/visa-warns-of-rise-in-gas-station-pos-cyberattacks/

Visa has announced in a release that cybercriminals are employing new tactics to steal credit card information from around the U.S.

While most are familiar with “skimming” attacks at gas stations, where criminals install a physical piece of scanning technology on an actual fuel dispenser, the new attacks are more complicated and require more technical knowledge.

Click link above to read more

AI Firm Breaches Facial Recognition At Airports, Stores

https://www.pymnts.com/news/security-and-risk/2019/ai-firm-breaches-facial-recognition-at-airports-stores/

Photos of faces and 3D masks have fooled facial recognition checkpoints at airports, as well as payment systems, but they can’t fool Apple’s Face ID systems, according to reports.

Kneron, an artificial intelligence (AI) company, did an experiment at different stores and airports that used facial recognition technology to see if it could fool the systems. In Asia, for example, the company used high-caliber 3D masks in an attempt to deceive payment systems like Alipay and WeChat. The testing team also was able to secure transportation hubs using a photo of a face on a phone screen.

Click link above to read more

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:

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


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