February 2nd, 2021

Try our February "LOVE SECURITY" Quiz

This week's stories:

Edmonton woman out $320 as e-transfer fraudsters cash in during pandemic

https://www.cbc.ca/news/gopublic/etransfer-fraud-pandemic-1.5889910

Alysia Lok may be the creator of a brand of sweet snacks, but says she's soured on how few protections can exist when e-transfers get hacked."I was just shocked and frustrated because I had no idea this could even happen," said the Edmonton entrepreneur.

When an e-transfer she expected from a client last November got redirected by a fraudster, the client's financial institution told Lok the money was gone for good — and not only that, it wasn't responsible for reimbursing her. "I started getting mad," said Lok. "They say e-transfer is 'fast, easy and secure.' So we used it, thinking that that's true."

Lok is one of a growing number of Canadians behind a surge in e-transfer transactions during the pandemic — as more people hunker down and use less cash, with fewer face-to-face retail interactions.

Click link above to read more

Companies that 'sweep data breaches under the rug' are paying a huge price

https://www.itworldcanada.com/article/data-breaches-still-swept-under-the-rug-despite-mandatory-reporting-says-kpmg/441459

Media coverage is still what prompts several Canadian organizations to respond effectively to data breaches, not the country's privacy legislation, according to KPMG's Imraan Bashir.

Some of the more embarrassing mishandling of private information in recent years – Bashir couldn't point out the stories or companies specifically – were pushed aside until the media got hold of it.

Bashir, partner and national leader of public sector cybersecurity, maintains that unless there's a colossal reset around how businesses in both the public and private sector view people's data, it will end up exposed or in the wrong hands. Organizations that sidestep responsibilities are losing the public's trust fast.

Click link above to read more

Canadian school board hit by 'cyber security incident'

https://www.itworldcanada.com/article/canadian-school-board-hit-by-cyber-security-incident/441527

One of the biggest public school boards in the country suffered what it called a "cyber security incident" earlier this week that encrypted some files.

The Peel District School Board, which covers the Ontario cities of Mississauga, Brampton and the town of Caledon serving about 155,000 students from kindergarten to grade 12 at more than 257 schools, made the admission in a tweet Thursday evening. The district is part of Peel Region, which is immediately west of Toronto.

As of last night, it had no evidence that "personal or sensitive information" was compromised.

On Friday morning the board's website was still unavailable, but its online classes were continuing.

Click link above to read more

Class-action lawsuit launched against TransLink for data breach in December

https://vancouversun.com/news/local-news/class-action-lawsuit-launched-against-translink-for-data-breach-in-december

Lawsuit alleges data breach resulted in 'loss, theft or compromise of highly sensitive personal information'

A class-action lawsuit has been launched against TransLink to compensate employees and retirees, and possibly others, affected by a huge ransomware data breach in December.

TransLink is named as the sole defendant in the notice of civil claim filed in B.C. Supreme Court alleging a data breach in early December "resulting in the loss, theft or compromise of highly sensitive personal information" of its employees "and other stakeholders."

Click link above to read more

International police effort takes down 'world's most dangerous' malware network

https://www.cnn.com/2021/01/28/tech/emotet-botnet-malware-takedown/index.html

Law enforcement authorities across several countries have taken down a network of what they describe as the "world's most dangerous malware."

The malware, Emotet, gained access to users' computers through infected email attachments, including documents purporting to be "invoices, shipping notices and information about Covid-19," European police agency Europol, which coordinated the effort, said in a statement Wednesday.

"The Emotet infrastructure essentially acted as a primary door opener for computer systems on a global scale," Europol said. "Once this unauthorised access was established, these were sold to other top-level criminal groups to deploy further illicit activities such as data theft and extortion."

Click link above to read more

3/4 of Americans have had to change password due to security breach

https://www.securitymagauzine.com/articles/94444-4-of-americans-have-had-to-change-password-due-to-security-breach

In advance of National Data Privacy Day this week (January 28), a new survey by iProov finds that 3/4 of respondents have had to change their password due to a security or data breach. That's up more than 10% over last year.

Additionally, more than two thirds of respondents have had to change their password two or more times due to a data breach.

Click link above to read more

Most Financial Services Have Suffered COVID-Linked Cyber-Attacks

https://www.infosecurity-magazine.com/news/financial-services-suffered-covid

Financial services firms were hit hard over the past year, with 70% experiencing a successful cyber-attack and most of these blaming COVID-related conditions for the incident, according to Keeper Security.

The password security firm commissioned the Ponemon Institute to poll over 370 UK IT security leaders in the sector, as part of a larger global study.

It revealed that the rapid shift to remote working forced on businesses during the pandemic provided threat actors with an opportunity to target remote workers.

Click link above to read more

Is Biden's $10B Enough to Make US Cybersecurity Great Again?

https://www.sdxcentral.com/articles/news/biden-10b-us-cybersecurity-great-again/2021/02/

President Joe Biden made cybersecurity a top priority for his administration even before he took office last month.

In December, shortly after threat researchers disclosed the SolarWinds hack that hit upwards of 250 government agencies and major tech companies, Biden pledged to "make dealing with this breach a top priority from the moment we take office."

"My administration will make cybersecurity a top priority at every level of government," the then-president-elect said in a statement.

However, Biden's emphasis on cybersecurity goes deeper than SolarWinds. "This was part of his campaign platform. It's not just something that's purely reactionary or politically motivated," said Lee Feldman, a strategy development manager for M12, which is Microsoft's corporate venture arm. "It was legitimately one of the things that he ran on, and some of his key personnel moves are good indicators of how big of a priority cybersecurity is going to be under the Biden administration."

Click link above to read more

Council Post: Cybersecurity Policing

https://www.forbes.com/sites/forbestechcouncil/2021/02/02/cybersecurity-policing/?sh=507a9a762aee

In today's world, it is not feasible for businesses to ignore cybersecurity. News about cybersecurity attacks and threats is common, including the legal challenges that develop due to these attacks. Enterprises must prioritize cybersecurity as an essential pillar of productivity and organizational development, though each business will have a unique approach to improving its protocols, depending on the nature and size of the business.

The following are the six most common areas for organizations to focus on when developing or updating cybersecurity policies and regulations. Please note that the precise wording of such policies may vary from organization to organization as per the business objectives and scope.

Click link above to read more

---

519 data breach notifications include 33 from Australian government entities

https://www.zdnet.com/article/519-data-breach-notifications-include-33-from-australian-government-entities/

Australian entities covered by the Privacy Act reported 519 instances of data breaches in the six months to December 2020, a 5% increase from the first half of the year.

Data breach notification to the Office of the Australian Information Commissioner (OAIC) became mandatory under the Notifiable Data Breaches (NDB) scheme in February 2018.

Since the mandate, health has been the most affected sector; the latest report [PDF] shows no change, with health accounting for 123 notifications, followed by finance with 83 notifications. The Australian government entered the top five sectors for the first time, accounting for 6% of the total, with 33 notifications.

Over half (57%) of respondents argued that cyber-attacks are increasing in severity as a result of work-from-home (WFH) and 41% argued that remote workers are putting the business at risk of a major data breach.

Click link above to read more

Threat Actor Dumps 1.9 Million Pixlr Records Online

https://www.infosecurity-magazine.com/news/threat-actor-dumps-19-million

A notorious threat actor appears to have published 1.9 million user records for the popular online photo editing site Pixlr, putting customers at risk of follow-on attacks.

"ShinyHunters" dumped the files over the weekend for free on an underground forum, claiming the site was breached at the same time as 123RF, which is owned by the same company, Inmagine.

Among the data up for grabs are email addresses, usernames, hashed passwords and users' countries.

So far there's been no word from the firm itself, despite the fact that these users could be at risk of phishing attacks, credential stuffing attempts and other fraud if not informed promptly.

Click link above to read more

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