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

July 5, 2022

Challenge yourself with our Travel Security quiz!

This past week's stories:

🍁 **Three trends defining the future of cybersecurity**
🍁 **Cyber spy agency targeted foreign extremists trying to recruit Canadians: report**

Norway targeted by cyber attack – security attack

Cybersecurity startups, once the VC darling, hammered by layoffs

Cybersecurity leaders are anticipating mass resignations within the year - here's why

Taking the guesswork out of cybersecurity

Explained: How cybercriminals are abusing messenger chatbots to steal Facebook credentials

Google enhances password manager to boost security across platforms

Hacker claims to have stolen 1 bln records of Chinese citizens from police

Google warns about hacker-for-hire services trying to phish users

UK Army's Twitter, YouTube accounts hacked to push crypto scam

Criminals use deepfake videos to interview for remote work

Three trends defining the future of cybersecurity

As Covid-19 enveloped the world in early 2020, Royal Bank of Canada (RBC), one of the world's top banks by market capitalization, joined organizations around the world in becoming a remote workplace. In less than a week, 85 percent of RBC's global workforce – almost 86,000 employees – were reconfiguring dining rooms into home offices and brushing up on videoconferencing software. Simultaneously, the bank's 17 million clients, some of whom had never used a digital platform, enrolled in online banking, switched to contactless payments and got comfortable e-signing personal documents.

RBC had been making steady strategic investments in digital transformation long before the global pandemic, but the goal posts shifted rapidly in a short time and catapulted the bank's strategy forward about 24 months. In fact, RBC is now seeing about 55 million digital banking transactions in a typical month.

https://betakit.com/three-trends-defining-the-future-of-cybersecurity/

Click above link to read more.

Back to top

Cyber spy agency targeted foreign extremists trying to recruit Canadians: report

Canada's electronic spy agency says it has used its arsenal to try to stop foreign extremists from recruiting Canadians and sharing violent material online.

The acknowledgement is nestled in the Communications Security Establishment's annual report made public Tuesday, which points to recent cases where it flexed its cyber muscles.

https://www.cbc.ca/news/politics/cse-extremism-active-operations-1.6503397

Click above link to read more.

Back to top

Norway targeted by cyber attack – security agency

A number of private and public institutions in Norway have been subjected to a so-called distributed denial-of-service (DDoS) cyber attack in the last 24 hours, the Norwegian NSM security authority said on Wednesday.

“A criminal pro-Russian group appears to be behind the attacks,” NSM said.

https://nationalpost.com/pmn/news-pmn/crime-pmn/norway-targeted-by-cyber-attack-security-agency

Click above link to read more.

Back to top

Cybersecurity startups, once the VC darling, hammered by layoffs

On the face of it, the cybersecurity sector is doing just fine. Demand for cybersecurity products remains high as cyberattacks continue to blight both public and private-sector businesses, and investor enthusiasm for all things cyber-related remains strong.

But while many expect the cybersecurity industry to weather the current economic storm better than most, not least due to the number of high-profile ransomware attacks and data breaches we're seeing each week, the sector is far from immune from the mass layoffs that are impacting every corner of the technology industry. Layoffs tracker Layoffs.fyi says almost 13,000 tech workers lost their jobs in June alone, compared to about 2,500 this time last year.

https://techcrunch.com/2022/06/29/cybersecurity-startups-layoffs/

Click above link to read more.

Back to top

Cybersecurity leaders are anticipating mass resignations within the year - here's why

Four in 10 UK cyber leaders say stress could push them to leave their job within the next year, according to a new study. Combined with the ongoing skills crisis, mass resignations could leave many sectors in a precarious situation.

Cybersecurity services company Bridewell surveyed 521 critical national infrastructure decision makers across multiple sectors, finding that 95% are experiencing factors that would make them likely to leave in the next 12 months. These leaders overwhelmingly attributed their desire to leave their position to two dominant causes: 42% say a cyber breach is inevitable and do not want it to tarnish their career, and 40% say stress and burnout are heavily impacting their personal lives.

https://www.zdnet.com/article/cybersecurity-leaders-are-anticipating-mass-resignations-within-the-year/

Click above link to read more.

Back to top

Taking the guesswork out of cybersecurity

Cyber security has become more dynamic, both in terms of the technology available to organizations and the wide range of threats that target them. In today's world, there is no scope for assuming whether a breach will happen, instead, it's a question of when.

In the current cyber security landscape, there is a wide array of vulnerabilities across the spectrum, waiting to be exploited by threat actors. What's more concerning is that illicit tools for exploiting those vulnerabilities are widely available on the dark web, whether it's sophisticated ransomware toolkits, social media reconnaissance, or phishing kits. So, cyber criminals can maximize their impact with minimum effort.

https://www.continuitycentral.com/index.php/news/technology/7440-taking-the-guesswork-out-of-cyber-security

Click above link to read more.

Back to top

Explained: How cybercriminals are abusing messenger chatbots to steal Facebook credentials

The researchers have explained that the objective of this campaign is to get hold of the user’s Facebook credentials and various other personal data. Representative Image Cybersecurity firm SpiderLabs has recently discovered a new phishing campaign that is using the chatbot software on Facebook Messenger, reports TechRadar. The researchers have explained that the objective of this campaign is to get hold of the user’s Facebook credentials and various other personal data.

According to the report, chatbots are hugely important for digital marketing and live support, so “cyber attackers are now abusing this feature.” Moreover, common users don’t usually suspect these contents, especially when it seems to come from a legitimate source, the report suggests.

https://newsazi.com/explained-how-cybercriminals-are-abusing-messenger-chatbots-to-steal-facebook-credentials-times-of-india/

Click above link to read more.

Back to top

Google enhances password manager to boost security across platforms

Google is rolling out key updates to its password management capabilities as part of an effort to boost security across multiple operating systems and browsers for mobile and desktop users, the company said in an announcement Thursday.

Google Password Manager users will now have the same unified experience whether using Chrome or Android, and iPhone users can now manage passwords through the iOS platform.

https://www.cybersecuritydive.com/news/google-password-manager-ios-android/626394/

Click above link to read more.

Back to top

Hacker claims to have stolen 1 bln records of Chinese citizens from police

A hacker has claimed to have procured a trove of personal information from the Shanghai police on one billion Chinese citizens, which tech experts say, if true, would be one of the biggest data breaches in history.

The anonymous internet user, identified as "ChinaDan", posted on hacker forum Breach Forums last week offering to sell the more than 23 terabytes (TB) of data for 10 bitcoin, equivalent to about $200,000.

https://www.reuters.com/world/china/hacker-claims-have-stolen-1-bln-records-chinese-citizens-police-2022-07-04/

Click above link to read more.

Back to top

Google warns about hacker-for-hire services trying to phish users

Google says it recently blocked dozens of malicious websites that so-called “hacker-for-hire” services were using to try to phish users.

The company published a blog post today intended to warn the public about the threat, which Google researchers have been tracking for years.

https://www.pcmag.com/news/google-warns-about-hacker-for-hire-services-trying-to-phish-users

Click above link to read more.

Back to top

UK Army’s Twitter, YouTube accounts hacked to push crypto scam

British Army's Twitter and YouTube accounts were hacked and altered to promote online crypto scams sometime yesterday.

Notably, the army's verified Twitter account began displaying fake NFTs and bogus crypto giveaway schemes.

https://www.bleepingcomputer.com/news/security/uk-army-s-twitter-youtube-accounts-hacked-to-push-crypto-scam/

Click above link to read more.

Back to top

Criminals use deepfake videos to interview for remote work

Security experts are on the alert for the next evolution of social engineering in business settings: deepfake employment interviews. The latest trend offers a glimpse into the future arsenal of criminals who use convincing, faked personae against business users to steal data and commit fraud.

The concern comes following a new advisory this week from the FBI Internet Crime Complaint Center (IC3), which warned of increased activity from fraudsters trying to game the online interview process for remote-work positions. The advisory said that criminals are using a combination of deepfake videos and stolen personal data to misrepresent themselves and gain employment in a range of work-from-home positions that include information technology, computer programming, database maintenance, and software-related job functions.

https://www.darkreading.com/attacks-breaches/criminals-deepfake-video-interview-remote-work

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