September 27, 2022

Get ready for Cyber Security Awareness Month Challenges this October!

Challenge yourself with our Ransomware Quiz!

This past week's stories:

- **B.C. regional government acknowledges cyber attack**
- **Older Canadians better at protecting against cyberattacks, poll says**
- **Calgary Parking investigation reveals more than 145,000 customers exposed during data breach**
- **Australia phones cyber-attack exposes personal data**
- **2K Games Support Desk Hacked, Phishing Emails Sent To Certain Players**
- **Ransomware Attacks Continue Increasing: 20% of All Reported Attacks Occurred in the Last 12 Months - New Survey**
- **Google removes malicious Chrome extensions with 1.4 million users**
- **Morgan Stanley to pay $35M after hard drives with 15M customers' personal data turn up in auction**
- **Fake sites fool Zoom users into downloading deadly code**
- **Ransomware operators might be dropping file encryption in favor of corrupting files**
- **Hackers Paralyze 911 Operations in Suffolk County, NY**
- **Mirai Security Announces The Launch of Its Free Cyber Security Awareness Toolkit**

B.C. regional government acknowledges cyber attack

A British Columbia municipality has acknowledged being the victim of a cyber attack just over two weeks ago.

The admission made today comes after the LockBit ransomware gang listed the Sunshine Coast Regional District on its data breach website.

https://www.itworldcanada.com/article/b-c-regional-government-acknowledges-cyber-attack/504480

Click above link to read more.

Back to top

Older Canadians better at protecting against cyberattacks, poll says

Is your online information secure? A new poll from Royal Bank of Canada has found half of the Canadians surveyed are worried about being a victim of a cyberattack, but it seems it's older people who are more likely to do something about it.

Most Canadians asked believe they are fairly knowledgeable about cyberattacks and the ways criminals target people online, however, the poll finds fewer are aware of the latest types of threats.

https://vancouver.citynews.ca/2022/09/27/canada-cyber-security-poll/

Click above link to read more.

Back to top

Calgary Parking investigation reveals more than 145,000 customers exposed during data breach

An investigation conducted by the Calgary Parking Authority, the city-operated agency that manages municipal parking services in the city, has revealed that the personal information of 145,895 customers was exposed for at least two months last year.

It's a revelation that the chair of the cybersecurity program at the Northern Alberta Institute of Technology is calling "shameful" and "negligent."

https://www.cbc.ca/news/canada/calgary/calgary-parking-authority-chris-blaschuk-data-breach-1.6596305
Click above link to read more.

Back to top

Australia phones cyber-attack exposes personal data

Australia's second-largest telecommunications company, Optus, has reported a cyber-attack.

The breach exposed customers' names, dates of birth, phone numbers and email addresses.

https://www.bbc.com/news/technology-62996101

Click above link to read more.

Back to top

2K Games Support Desk Hacked, Phishing Emails Sent To Certain Players

Following Rockstar's GTA 6 leaks, a fellow Take-Two brand is facing a security threat. 2K Games took to Twitter to put out a warning message: One of the company's customer support help desks was hacked and malicious links were sent to certain players.

"Please do not open any emails or click on any links that you receive from the 2K Games support account." 2K said. If you have already clicked on a suspicious link, 2K recommends that you reset passwords stored in web browsers, enable multi-factor authentication, run an antivirus program, and check account settings to see if any forwarding rules have been newly added.

https://www.gamespot.com/articles/2k-games-support-desk-hacked-phishing-emails-sent-to-certain-players/1100-6507702/

Click above link to read more.

Back to top

Ransomware Attacks Continue Increasing: 20% of All Reported Attacks Occurred in the Last 12 Months - New Survey

Nearly a quarter of businesses have suffered a ransomware attack, with a fifth occurring in the past 12 months, according to a latest annual report from cybersecurity specialist Hornetsecurity.

The 2022 Ransomware Report, which surveyed over 2,000 IT leaders, revealed that 24% have been victims of a ransomware attack, with one in five (20%) attacks happening in the last year.

https://www.prnewswire.com/news-releases/ransomware-attacks-continue-increasing-20-of-all-reported-attacks-occurred-in-the-last-12-months--new-survey-301632488.html

Click above link to read more.

Back to top

Google removes malicious Chrome extensions with 1.4 million users

By now you probably know that you need to exercise caution when installing new programs on your computer. But savvy web users know that the same thing applies to web browser extensions — which are, in a way, merely smaller programs on a more specific platform. Such is the case with a series of five Chrome browser extensions Google recently removed from its official Chrome Web Store repository.

The five extensions had been installed by a combined 1.4 million users before Google took them down. According to a report by McAfee security researchers (via Ars Technica), the extensions kept a list of every website visited by the user, along with their location down to the city and county. The extension would then inject custom Javascript ads onto certain websites, earning the developers some ill-gotten advertising revenue. In an especially tricky twist, some of the extensions would wait fifteen days to inject its advertising, making the source of the problem all the harder to track down.

https://www.pcworld.com/article/919764/google-removes-malicious-chrome-extensions-with-millions-of-users.html

Click above link to read more.

Back to top

Morgan Stanley to pay $35M after hard drives with 15M customers' personal data turn up in auction

The U.S. Securities and Exchange Commission has agreed to settle charges against Morgan Stanley Smith Barney (MSSB) for its "astonishing" failure to protect the personal identifying information of some 15 million customers.

MSSB, now known as Morgan Stanley Wealth Management, is the wealth and asset management division of banking giant Morgan Stanley, which this week agreed to pay $35 million to settle allegations that it failed to properly dispose of hard drives and servers containing its customers' personal data over a five-year period as far back as 2015.

https://techcrunch.com/2022/09/21/morgan-stanley-hard-drives-data-breach/

Click above link to read more.

Back to top

Fake sites fool Zoom users into downloading deadly code

Beware the Zoom site you don't recognize, as a criminal gang is creating multiple fake versions aimed at luring users to download malware that can steal banking data, IP addresses, and other information.

Threat researchers at cybersecurity firm Cyble found six fake Zoom sites offering applications that, if clicked on, will download the Vidar Stealer malware, which also grabs lots of other goodies. The fake Zoom sites are part of a wider info-stealing effort, according to the Cyble Research and Intelligence Lab (CRIL).

https://www.theregister.com/2022/09/22/zoom_malware_infosteal_cyble/

Click above link to read more.

Back to top

Ransomware operators might be dropping file encryption in favor of corrupting files

Ransomware started out many years as scams where users were being tricked into paying fictitious fines for allegedly engaging in illegal online behavior or, in more serious cases, were blackmailed with compromising videos taken through their webcams by malware. The threat has since come a long way, moving from consumers to enterprises, adding data leak threats on the side and sometimes distributed denial-of-service (DDoS) blackmail.

The attacks have become so widespread that they now impact all types of organizations and even entire national governments. The cybercriminal groups behind them are well organized, sophisticated, and even innovative, always coming up with new extortion techniques that could earn them more money. But sometimes, the best way to achieve something is not to complexity but to simplify and this seems to be the case in new attacks seen by researchers from security firms Stairwell and Cyderes where known ransomware actors opted to destroy files instead of encrypting them.

https://www.csoonline.com/article/3674848/ransomware-operators-might-be-dropping-file-encryption-in-favor-of-corrupting-files.html

Click above link to read more.

Back to top

Hackers Paralyze 911 Operations in Suffolk County, NY

A Sept. 8 ransomware attack on Suffolk County government systems in New York continues to wreak havoc on citizens of the area, driving overwhelmed 911 operators working without the aid of computers to call for backup.

The ransomware attack means that emergency operators are working with pen and paper, then making phone calls to dispatch officers to send help, according to New York's NBC affiliate. The Suffolk County Police Department has asked the New York Police Department for help handling the calls. In response, the NYPD will add five extra officers per shift to help, NBC New York reported.

https://www.darkreading.com/attacks-breaches/hackers-paralyze-911-operations-suffolk-county-ny

Click above link to read more.

Back to top

Mirai Security Announces The Launch of Its Free Cyber Security Awareness Toolkit

Mirai Security, one of Canada's leading cybersecurity firms, today announced the release of its new cybersecurity awareness toolkit in preparation for Cybersecurity Awareness Month 2022 in October. The BC cybersecurity consulting authority is thrilled to provide this free, ungated toolkit to bolster security awareness within organizations and throughout the general public.

The Toolkit: A Comprehensive Guide to Building a Better Security Culture

https://financialpost.com/pmn/press-releases-pmn/business-wire-news-releases-pmn/mirai-security-announces-the-launch-of-its-free-cyber-security-awareness-toolkit
Click above link to read more.

Back to top