March 9th, 2021

Try our March Fraud Prevention Quiz

This week's stories:

Girl Guides of Canada and BlackBerry Announce Success of Joint Cybersecurity Education Program

'Digital Defenders' crests awarded to 5,600+ cybersavvy girls

To mark International Women's Day, Girl Guides of Canada-Guides du Canada (GGC) and BlackBerry Limited (NYSE: BB; TSX: BB) today announced the success of their joint cybersecurity skills-based program, with more than 5,600 GGC members across the country earning Digital Defenders crests; proof of their newfound cyber-smarts.

Girl Guides of Canada-Guides du Canada (GGC) and BlackBerry Limited today announced the success of their joint cybersecurity skills-based program, with more than 5,600 GGC members across the country earning Digital Defenders crests.

Girl Guides of Canada-Guides du Canada (GGC) and BlackBerry Limited today announced the success of their joint cybersecurity skills-based program, with more than 5,600 GGC members across the country earning Digital Defenders crests.

https://finance.yahoo.com/news/girl-guides-canada-blackberry-announce-130000277.html

Click link above to read more

How vaccine-related phishing attacks are posing a greater threat to organizations

Scammers are launching more malicious campaigns designed to take advantage of the anxiety and confusion over the COVID-19 vaccines.

The rollout of coronavirus vaccines around the world is certainly welcome news following a year grappling with the deadly pandemic. But vaccine deployment has encountered bumps in the road as many people are still uncertain over when, where and how to get their shots. That confusion has been ripe for exploitation by cybercriminals, triggering an increase in related phishing scams, according to Check Point Research and Barracuda Networks.

In a blog post published last week, Check Point revealed an increase in the number of domains with the word “vaccine” in their titles. Over the past four months, the volume of new vaccine-related domains shot up by 7,056, of which 294 have been deemed potentially dangerous by Check Point.

Pointing to one example, Check Point said it recently discovered a malicious website impersonating the U.S. Centers for Disease Control and Prevention and promising vaccine information. To get the alleged information, visitors are asked to enter their Microsoft credentials, which the attackers naturally capture.

https://nationalcybersecuritynews.today/how-vaccine-related-phishing-attacks-are-posing-a-greater-threat-to-organizations-phishing-scams-phishing-scams/

Click link above to read more

80% of senior IT leaders see cybersecurity protection deficits

A lack of confidence in companies' defenses is prompting 91% of organizations to boost 2021 budgets, according to a new IDG/Insight Enterprises study.

Nearly 80% of senior IT and IT security leaders believe their organizations lack sufficient protection against cyberattacks despite increased IT security investments made in 2020 to deal with distributed IT and work-from-home challenges, according to a new IDG survey commissioned by Insight Enterprises.

That high level of concern over the ability to withstand cyber threats in today's complex IT environment is causing 91% of organizations to increase their cybersecurity budgets in 2021, nearly matching the 96% that boosted IT security spending in 2020, according to the survey by Insight's Cloud + Data Center Transformation team.

The survey examined the impact of the distributed IT landscape and pandemic-related transition to a remote workforce on IT security, including shifts in modernization priorities, projects undertaken in 2020 and major obstacles faced in strengthening cybersecurity defenses.

https://www.techrepublic.com/article/80-of-senior-it-leaders-see-cybersecurity-protection-deficits/

Click link above to read more

How the Microsoft Exchange hack could impact your organization

Cybercriminals are racing to exploit four zero-day bugs in Exchange before more organizations can patch them.

Organizations that run Microsoft Exchange Server are being urged to apply several bug fixes to the program in response to a hack from a Chinese cybercriminal group. The attack has sparked concern among everyone from security experts to the White House.

Early last week, Microsoft revealed that a China-based group called Hafnium has been launching cyberattacks against organizations by exploiting four zero-day vulnerabilities in on-premises versions of its Exchange Server software. The attacks are being carried out in three steps, according to Microsoft.

First, the group is able to gain access to an Exchange server either by using stolen account credentials or by using the vulnerabilities to masquerade as someone who should have access. Second, the group is able to control the compromised server remotely by creating a web shell, a piece of malicious code that gives attackers remote administrative access. Third, the group uses the remote access to steal data from an organization's network.

https://www.techrepublic.com/article/how-the-microsoft-exchange-hack-could-impact-your-organization/

Click link above to read more

Apple Issues Patch for Remote Hacking Bug Affecting Billions of its Devices

Apple has released out-of-band patches for iOS, macOS, watchOS, and Safari web browser to address a security flaw that could allow attackers to run arbitrary code on devices via malicious web content.

Tracked as CVE-2021-1844, the vulnerability was discovered and reported to the company by Clément Lecigne of Google's Threat Analysis Group and Alison Huffman of Microsoft Browser Vulnerability Research.

According to the update notes posted by Apple, the flaw stems from a memory corruption issue that could lead to arbitrary code execution when processing specially crafted web content. The company said the problem was addressed with "improved validation."

https://thehackernews.com/2021/03/apple-issues-patch-for-remote-hacking.html

Click link above to read more

Microsoft Edge Legacy will now prompt you to install Chromium Edge

Microsoft Edge Legacy has officially reached the end of life today, and starting tomorrow, the web browser will begin displaying notifications telling users to switch to the new Chromium-based Microsoft Edge.

Starting March 10th, 2021, users who still use Microsoft Edge Legacy will be shown a notification at the bottom of the screen stating:

“This version of Microsoft Edge is no longer supported or receiving security updates. Download the new version of Microsoft Edge today.”

https://nationalcybersecuritynews.today/microsoft-edge-legacy-will-now-prompt-you-to-install-chromium-edge-firefox-firefoxsecurity/

Click link above to read more

Airlines warn passengers of data breach after aviation tech supplier is hit by cyberattack

Sita, which provides IT of services to 90% of the world's airlines, warns of "data security incident" after falling victim to a "highly sophisticated attack"

Global aviation industry IT supplier SITA has confirmed it has fallen victim to a cyberattack, with hackers gaining access to personal information of airline passengers.

The information technology and communications company, which claims to serve around 90% of the world's airlines, said that a cyberattack on February 24, 2021 led to "data security incident" involving passenger data that was stored on SITA Passenger Service System Inc. servers located at Atlanta, Georgia in the United States.

A statement by SITA describes the incident as a "highly sophisticated attack" and said that the company "acted swiftly" to contain the incident, which still remains under investigation by SITA's Security Incident Response Team, alongside external cybersecurity experts.

https://www.zdnet.com/article/airlines-warn-passengers-of-data-breach-after-aviation-tech-supplier-is-hit-by-cyberattack/

Click link above to read more

Retailers battle bots as new Yeezy shoes debut in March

Shopping bots are now the biggest, and for some, most enraging impediment to shoppers looking for the hottest items online, beating out everyday people thanks to powerful technology that has been democratized by sites like Cybersole, Kodai, GaneshBot and more. Those using bots then resell the goods for double, and sometimes triple, the price.

Recently, the new Adidas Yeezy Boost 700 "Sun" shoes from Kanye West made their debut, raising concerns that bots were likely on a shopping spree as they traditionally are during weeks when a hot new brand is launched.

Researchers with cybersecurity company PerimeterX found evidence of "sneaker bots" dominating checkout pages. Attackers typically use monitoring tools to check a retailer's inventory several days before the launch day and even try to add the proposed shoe to the cart, to shorten the purchase flow and to bypass innocent buyers, according to PerimeterX CMO Kim DeCarlis.

https://www.techrepublic.com/article/retailers-battle-bots-as-new-yeezy-shoes-debut-in-march/

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:

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

OCIOSecurity@gov.bc.ca