June 14, 2022

Challenge yourself with our Phishing quiz!

This past week's stories:

- **New cybersecurity bill to require mandatory reporting of ransomware, other attacks**
- **Nearly half of Sask. school divisions vulnerable to cyberattack, auditor says**
- **Cybersecurity course for disadvantaged youth now offered by Canadian agency**
- **What should you do if you've been scammed?**
- **Hacking scenarios: How hackers choose their victims**
- **More than 90% of cyberattacks are made possible by human error**
- **India's loan scams leave victims scared for their lives**
- **National Cyber Security Centre certify master's degree**
- **Millions of Facebook users' credentials harvested using legitimate app services**
- **MIT researchers discover new flaw in Apple M1 CPUs that can't be patched**
- **How to make business practices that support cybersecurity response**
- **Monkeypox threatens infection – of your computer**
- **45% of cybersecurity pros are considering quitting the industry due to stress**

New cybersecurity bill to require mandatory reporting of ransomware, other attacks

Businesses and other private-sector organizations would be required to report ransomware incidents and other cyberattacks to the government under a federal bill to be tabled today.

The legislation is intended to flesh out Liberal government efforts to protect critical infrastructure following last month's announcement that Chinese vendors Huawei Technologies and ZTE will be banned from Canada's next-generation mobile networks.

https://globalnews.ca/news/8918652/canada-cybersecurity-bill/

Click above link to read more.

Back to top

Nearly half of Sask. school divisions vulnerable to cyberattack, auditor says

In her latest annual report, which was released Tuesday, Saskatchewan's provincial auditor says she found 13 of Saskatchewan's 27 school divisions were more vulnerable to cyberattack than they need be due to the use of outdated software.

Tara Clemett's research shows that in August of 2021, 13 school divisions using the same financial IT software had not completely updated their systems with available security patches. Patches are often issued when particular vulnerabilities are identified by service providers.

https://globalnews.ca/news/8905666/saskatchewan-school-divisions-vulnerable-cyberattack/

Click above link to read more.

Back to top

Cybersecurity course for disadvantaged youth now offered by Canadian agency

Post-secondary Canadian institutions are increasingly offering cybersecurity courses to help fill the demand for infosec pros.

The latest is a Toronto-area not-for profit agency called Youth Employment Services (YES) that trains disadvantaged and vulnerable youth aged 15 to 29. Next month it starts a cybersecurity course with paid training in conjunction with IBM. Graduates of the free 13-week course will receive an IBM Cybersecurity Analyst Professional Certificate.

https://financialpost.com/technology/cybersecurity-course-for-disadvantaged-youth-now-offered-by-canadian-agency-3

Click above link to read more.

Back to top

What should you do if you've been scammed?

The Canadian Anti-Fraud Centre states that in 2021, there were 106,875 reported cases of fraud. As of April 30, 2022, there have already been 29,294 cases this year.

If you find yourself the victim, what rights and options do you have?

https://vancouversun.com/moneywise-pro/growing-money/what-should-you-do-if-youve-been-scammed?r

Click above link to read more.

Back to top

Hacking scenarios: How hackers choose their victims

Enforcing the "double-extortion" technique aka pay-now-or-get-breached emerged as a head-turner last year.

May 6th, 2022 is a recent example.

The State Department said the Conti strain of ransomware was the most costly in terms of payments made by victims as of January.

https://thehackernews.com/2022/06/hacking-scenarios-how-hackers-choose.html

Click above link to read more.

Back to top

More than 90% of cyberattacks are made possible by human error

In a ransomware attack, a company's computer systems are locked, and the attacker demands a ransom in cryptocurrency in return for unlocking the system. Malware infects a network of objects connected to the Internet of Things to steal the personal data of its users. Talking about cybersecurity is talking about technology. However, it is increasingly common to study cyber risk as part of an interdisciplinary approach. After all, threats are technological, but they also have to do with behavioral, social and ethical factors.

https://techxplore.com/news/2022-06-cyberattacks-human-error.html

Click above link to read more.

Back to top

India's loan scams leave victims scared for their lives

When Raj took out a loan for $110 (£87) in March, he thought it would swiftly solve his financial problems, instead it has made his life much, much worse.

The Pune-based man had been lured into one of India's many digital loan scams.

Like many, Raj (not his real name), was attracted by the quick and easy loan approval process. All he had to do was download an app to his phone and supply a copy of his identity card to qualify.

https://www.bbc.com/news/business-61564038

Click above link to read more.

Back to top

National Cyber Security Centre certify master's degree

The National Cyber Security Centre (NCSC), a part of GCHQ, has certified the master's degree in cybersecurity at University of Gloucestershire as part of its programme to recognise high-quality courses.

The University's NCSC-certified MSc Cyber Security course is designed for those who would like to develop a career as a cybersecurity professional, or to take a leading technical or managerial role.

https://edtechnology.co.uk/cybersecurity/national-cyber-security-centre-certify-masters-degree/

Click above link to read more.

Back to top

Millions of Facebook users' credentials harvested using legitimate app services

AI-driven cybersecurity vendor PIXM Security recently stumbled upon a stealth phishing campaign exploiting Facebook user accounts through legitimate online services. With possible origins in Columbia, the phishers have earned tens of millions of dollars in revenue through ad referrals through the campaign.

The phishers have been harvesting user credentials from Facebook and have impacted millions of users. The New York-based cybersecurity company detailed the technical and operational aspects of this malicious campaign involving phishers avoiding detection using legitimate online services.

https://www.toolbox.com/it-security/web-security/news/facebook-phishing-campaign-earning-ad-revenue/

Click above link to read more.

Back to top

MIT researchers discover new flaw in Apple M1 CPUs that can't be patched

A novel hardware attack dubbed PACMAN has been demonstrated against Apple's M1 processor chipsets, potentially arming a malicious actor with the capability to gain arbitrary code execution on macOS systems.

It leverages "speculative execution attacks to bypass an important memory protection mechanism, ARM Pointer Authentication, a security feature that is used to enforce pointer integrity," MIT researchers Joseph Ravichandran, Weon Taek Na, Jay Lang, and Mengjia Yan said in a new paper.

https://thehackernews.com/2022/06/mit-researchers-discover-new-flaw-in.html

Click above link to read more.

Back to top

How to make business practices that support cybersecurity response

Scottish author Robert Burns wrote in the poem “To a Mouse,” “The best-laid schemes o’ mice an’ men. Gang aft a-gley.” You may better know the saying in its more common form, “The best-laid plans of mice and men often go awry.”

This saying may resonate with incident responders, business continuity planners and crisis managers. They know all too well that all plans may be useless after the first shot is fired. But, as former President Dwight D. Eisenhower said, “In planning for battle, I have always found that plans are useless, but planning is indispensable.” To be ready, start with finding out which business practices and processes can impact response and build a governance structure that supports a resilient organization.

https://securityintelligence.com/articles/business-practices-support-cybersecurity-response/

Click above link to read more.

Back to top

Monkeypox threatens infection – of your computer

Mimecast has discovered a new email phishing campaign that aims to use the emerging monkeypox outbreak to trick employees into sharing their personal details.

“Monkeypox is high on the news agenda so it comes as no surprise that cybercriminals are exploiting it,” says Tim Campbell, head of threat intelligence at Mimecast. “Cybercriminals adjust their phishing campaigns to be as timely and relevant as possible, using traditional attack methods to exploit current events in an attempt to lure busy and distracted people to engage with links in emails, applications or texts.

https://gadget.co.za/monkeypox-threatens-infection-of-your-computer/

Click above link to read more.

Back to top

45% of cybersecurity pros are considering quitting the industry due to stress

Deep Instinct released the third edition of its annual Voice of SecOps Report, focused on the increasing and unsustainable stress levels among 1,000 C-suite and senior cybersecurity professionals across all industries and roles. The research found that 45% of respondents have considered quitting the industry due to stress, with the primary issues being an unrelenting threat from ransomware and the expectations to always be on call or available.

https://www.helpnetsecurity.com/2022/06/13/cybersecurity-professionals-stress-levels/

Click above link to read more.

Back to top

---

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