June 7, 2022

Challenge yourself with our Phishing quiz!

This past week's stories:

- **Ask an expert: Social media cyber security**
- **Bad news: The cybersecurity skills crisis is about to get even worse**
- **Empathy: The overlooked ingredient in cybersecurity**
- **Researchers find critical bug in UNISOC smartphone chip**
- **Russia-linked ransomware groups are changing tactics to dodge crackdowns**
- **Forget fake news, it's all about scams on social media**
- **Customer support impersonation scams on Twitter**
- **NHS Digital launch new cyber security toolkit**
- **Russia's government website hacked with pro-Ukraine message displayed instead**
- **Chinese LuoYu hackers using man-on-the-side attacks to deploy WinDealer backdoor**
- **Keyboard-patterned passwords flagged in Taiwan's cybersecurity report**
- **Bored Ape Yacht Club, Otherside NFTs stolen in Discord server hack**
- **Microsoft Seizes 41 domains used in spear-phishing attacks by Bohrium hackers**

Ask an expert: Social media cyber security

Derek Manky, Chief Security Strategist at Fortinet, shares some tips and tricks to protect yourself on social media. He also looks at some of the most common mistakes he sees from users.

https://globalnews.ca/video/8898062/ask-an-expert-social-media-cyber-security

Click above link to read more.

Back to top

Bad news: The cybersecurity skills crisis is about to get even worse

Nearly a third of the cybersecurity workforce is planning to leave the industry in the near future**,** new research suggests, leaving organizations in a troubling position as the threat landscape evolves "at an alarming rate".

Cybersecurity firm Trellix commissioned a survey of 1,000 cybersecurity professionals globally and found that 30% are planning to change professions within two or more years**.** Organizations are already facing cybersecurity skills shortages, with not enough people having the skills and qualifications required to keep IT systems secure from breaches and other security threats.

https://www.zdnet.com/article/bad-news-the-cybersecurity-skills-crisis-is-about-to-get-even-worse/

Click above link to read more.

Back to top

Empathy: The overlooked ingredient in cybersecurity

Technological innovation is moving at the speed of life. We live in a world infused with artificially intelligent sensors that cross biological, physical and digital boundaries. Not surprisingly, cybersecurity and GRC workforces are struggling to keep pace. The people, processes and technologies that make our new world go round require a very different approach toward protection and defense.

The problems we have are primitive, systemic and require transformative thinking and approaches. To design and build the cybersecurity workforces of the future, we must have a clear understanding of our current state, which includes an analysis of our emotional state – a deeper dive into our humanity.

https://www.infosecurity-magazine.com/blogs/empathy-overlooked-cybersecurity/

Click above link to read more.

Back to top

Researchers find critical bug in UNISOC smartphone chip

Cyber-security researchers on Thursday reported a critical security vulnerability in UNISOC's smartphone chip being used for cellular communication in 11 per cent of the world's smartphones.

Left unpatched, an attacker could exploit the vulnerability to neutralize or block cellular communication, according to Check-Point Research, a cybersecurity firm.

https://telecom.economictimes.indiatimes.com/news/researchers-find-critical-bug-in-unisoc-smartphone-chip/91965413

Click above link to read more.

Back to top

Russia-linked ransomware groups are changing tactics to dodge crackdowns

Russia-linked ransomware groups are splitting into smaller cells or cycling through different types of malware in attempts to evade a growing array of U.S. sanctions and law-enforcement pressure, cybersecurity experts say.

After the U.S. in 2019 sanctioned a Russia-based group known as Evil Corp, which Washington accused of stealing over $100 million from more than 300 banks, hackers believed to be affiliated with the gang switched its operating model, according to a report published Thursday by security firm Mandiant Inc. The individuals ditched Evil Corp's bespoke malware and rotated between several related variants.

https://www.wsj.com/articles/russia-linked-ransomware-groups-are-changing-tactics-to-dodge-crackdowns-11654178400?mod=business_minor_pos4

Click above link to read more.

Back to top

Forget fake news, it's all about scams on social media

Social media scams continue to cause problems for both consumers and enterprises today. While businesses recognize the need to leverage social media as a sales tool and connect with customers, the problems that come with it can be too overwhelming for them.

Over the years, social media scams have been increasing, with victims losing more than just funds. In fact, researchers from Group -IB see that the scam industry is becoming more structured and involves more and more parties divided into hierarchical groups. The number of such groups jumped to a record high of 390, which is 3.5 times more than last year when the maximum number of active groups was close to 110.

https://techwireasia.com/2022/06/forget-fake-news-its-all-about-scams-on-social-media/

Click above link to read more.

Back to top

Customer support impersonation scams on Twitter

Many companies use social media platforms as an outlet to manage their relations with customers, troubleshoot user problems, and answer their queries.

Twitter is one of the key platforms where users can tag the brand's handle with the troubles they're facing or feedback about the services. The brand's Twitter handle tries to troubleshoot the problem or refers the user to a support page or link where the user can raise requests.

https://securityboulevard.com/2022/06/customer-support-impersonation-scams-on-twitter/

Click above link to read more.

Back to top

NHS Digital launch new cyber security toolkit

NHS Digital have updated their security awareness toolkit to include specialised support and advice for social care organisations.

The toolkit, named Keep I.T. Confidential, aims to improve staff knowledge on a variety of cyber security concerns such as, phishing, data sharing, unlocked screens and weak passwords.

https://www.nationalhealthexecutive.com/articles/nhs-digital-launch-social-care-cyber-security-toolkit

Click above link to read more.

Back to top

Russia’s government website hacked with pro-Ukraine message displayed instead

A Russian government website appears to have been hacked over the weekend, causing an Internet search for the site to lead to a "Glory to Ukraine" sign in Ukrainian.

Russia's Ministry of Construction, Housing and Utilities website was targeted after many of the country's state-owned companies and news organisations suffered hacking attempts since the Russian government's invasion of Ukraine on February 24.

https://www.euronews.com/next/2022/06/06/russia-s-government-website-hacked-with-pro-ukraine-message-displayed-instead

Click above link to read more.

Back to top

Chinese LuoYu hackers using man-on-the-side attacks to deploy WinDealer backdoor

An "extremely sophisticated" Chinese-speaking advanced persistent threat (APT) actor dubbed LuoYu has been observed using a malicious Windows tool called WinDealer that's delivered by means of man-on-the-side attacks.

"This groundbreaking development allows the actor to modify network traffic in-transit to insert malicious payloads," Russian cybersecurity company Kaspersky said in a new report. "Such attacks are especially dangerous and devastating because they do not require any interaction with the target to lead to a successful infection."

https://thehackernews.com/2022/06/chinese-luoyu-hackers-using-man-on-side.html

Click above link to read more.

Back to top

Keyboard-patterned passwords flagged in Taiwan's cybersecurity report

Keyboard sequence passwords have been found to be a vulnerability easily exploited in the latest Cabinet-released cybersecurity report on government agencies in Taiwan.

The monthly report for April suggested a hack into email accounts at a government unit involving leaked passwords, many of which were keyboard-patterned combinations such as "1qaz@WSX." Such passwords, though consisting of a mix of characters and symbols, can be cracked easily by hackers.

https://www.taiwannews.com.tw/en/news/4559969

Click above link to read more.

Back to top

Bored Ape Yacht Club, Otherside NFTs stolen in Discord server hack

Hackers reportedly stole over $257,000 in Ethereum and thirty-two NFTs after the Yuga Lab's Bored Ape Yacht Club and Otherside Metaverse Discord servers were compromised to post a phishing scam.

Earlier this morning, the Discord account for a Yuga Labs community manager was allegedly hacked to post a phishing scam on the company's Discord servers.

https://www.bleepingcomputer.com/news/security/bored-ape-yacht-club-otherside-nfts-stolen-in-discord-server-hack/

Click above link to read more.

Back to top

Microsoft Seizes 41 domains used in spear-phishing attacks by Bohrium hackers

Microsoft's Digital Crimes Unit (DCU) last week disclosed that it had taken legal proceedings against an Iranian threat actor dubbed Bohrium in connection with a spear-phishing operation.

The adversarial collective is said to have targeted entities in tech, transportation, government, and education sectors located in the U.S., Middle East, and India.

https://thehackernews.com/2022/06/microsoft-seizes-41-domains-used-in.html

Click above link to read more.

Back to top

To learn more about information security issues and best practices, visit us at:

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

OCIOSecurity@gov.bc.ca