March 26, 2024

Challenge yourself with our RFID Skimming Quiz!

Cybersecurity theme of the week: **Multi-Factor Authentication**

✪ Check out our **MFA Quiz** to learn more.

Wonder what you can do to better protect yourself using MFA?

All Users	Technical Users	Business Owners
Ensure that you are taking advantage of multi-factor authentication (MFA) with your accounts and services whenever it is available. Including social media, banking, subscriptions services and any apps you may use.	Include incident response exercises where MFA is bypassed. Take detailed notes to identify lessons learned and areas for improvement.	Ask your teams how MFA can be bypassed and what measures they are taking to prevent it from occurring. What else can we do to secure our accounts?

This past week's stories:

Cybersecurity breach at Giant Tiger involves customer's personal information
Huntsville provides update on services available after cyber security incident
New 'Loop DoS' attack impacts hundreds of thousands of systems
French Football Federation (FFF) allegedly hacked: Hackers selling 10M records in dark web
✪ **Pokémon resets users password following hacking attempts**
Russia hackers using TinyTurla-NG to breach European NGO's systems
EU Policy. Commission to work on standards for high-risk IoT products under cyber rules
'New wave of cybersecurity attack:' Deepfake AI poses threat on social media
Britain says China hacked electoral watchdog, targeted lawmaker emails
Threat actor claims to have 600,000 passenger data of Kuwait Airways

The 10 best (and worst) countries for cybersecurity
'PhantomBlu' cyberattackers backdoor Microsoft Office users via OLE

Cybersecurity breach at Giant Tiger involves customer's personal information

Canadian discount store chain Giant Tiger is warning of a recent cybersecurity breach involving customer’s information.

https://atlantic.ctvnews.ca/giant-tiger-warns-of-cybersecurity-breach-involving-customer-information-1.6819627

Click above link to read more.

Back to top

Huntsville provides update on services available after cyber security incident

The Town of Huntsville says the cybersecurity incident is still affecting certain systems and online applications and they advise you to Contact Town Hall Customer Service at 705-789-1751 for inquiries about current services.

https://muskokaradio.com/news/article/huntsville-provides-update-on-services-available-after-cyber-security-incident

Click above link to read more.

Back to top

New 'Loop DoS' attack impacts hundreds of thousands of systems

Story text. A novel denial-of-service (DoS) attack vector has been found to target application-layer protocols based on User Datagram Protocol (UDP), putting hundreds of thousands of hosts likely at risk.

Called Loop DoS attacks, the approach pairs "servers of these protocols in such a way that they communicate with each other indefinitely," researchers from the CISPA Helmholtz-Center for Information Security said.

https://thehackernews.com/2024/03/new-loop-dos-attack-impacts-hundreds-of.html

Click above link to read more.

Back to top

French Football Federation (FFF) allegedly hacked: Hackers selling 10M records in dark web

The Fédération Française de Football (FFF) has been informed of allegations regarding a potential security breach within their systems.

https://cybersecuritynews.com/french-football-federation-fff-allegedly-hacked/

Click above link to read more.

Back to top

✪ Pokémon resets users password following hacking attempts

The Pokémon Company has taken decisive action to safeguard its users by resetting passwords after detecting unauthorized hacking attempts.

https://cybersecuritynews.com/pokemon-hacking-attempts/

Click above link to read more.

Back to top

Russia hackers using TinyTurla-NG to breach European NGO's systems

The Russia-linked threat actor known as Turla infected several systems belonging to an unnamed European non-governmental organization (NGO) in order to deploy a backdoor called TinyTurla-NG.

https://thehackernews.com/2024/03/russia-hackers-using-tinyturla-ng-to.html

Click above link to read more.

Back to top

EU Policy. Commission to work on standards for high-risk IoT products under cyber rules

The European Commission will work on cybersecurity standardisation requests for high-risk connected products as soon as the Cyber Resilience Act (CRA) is fully adopted, a commission official said today (21 March).

https://www.euronews.com/next/2024/03/21/commission-to-work-on-standards-for-high-risk-iot-products-under-cyber-rules

Click above link to read more.

Back to top

‘New wave of cybersecurity attack:’ Deepfake AI poses threat on social media

With the presidential election year upon us, the impact of audio and video deepfake AI has become the hot conversation in 2024.

https://www.clickorlando.com/news/local/2024/03/25/new-wave-of-cybersecurity-attack-deepfake-ai-poses-threat-on-social-media/

Click above link to read more.

Back to top

Britain says China hacked electoral watchdog, targeted lawmaker emails

Britain on Monday accused Chinese hackers of trying to break into email accounts of British lawmakers who were critical of China and said a separate Chinese entity was behind a hack of its electoral watchdog that compromised millions of people's data.

https://www.reuters.com/world/uk/uk-deputy-pm-set-address-lawmakers-chinese-cyber-security-threat-2024-03-24/

Click above link to read more.

Back to top

Threat actor claims to have 600,000 passenger data of Kuwait Airways

A threat actor has claimed responsibility for a massive data breach affecting Kuwait Airways.

https://cybersecuritynews.com/claims-passenger-data-airways/

Click above link to read more.

Back to top

The 10 best (and worst) countries for cybersecurity

A 2023 Harvard Business study has revealed that data breaches in the US are at an “all time high”, increasing by 20 per cent in the first three quarters of 2023 compared to 2022. The picture was similar around the globe where attacks were particularly focused on the UK, Australia and Canada. In the Middle East ransomware gang activity grew by 77 per cent during the same year.

https://www.sciencefocus.com/news/the-10-best-and-worst-countries-for-cybersecurity

Click above link to read more.

Back to top

'PhantomBlu' cyberattackers backdoor Microsoft Office users via OLE

A malicious email campaign is targeting hundreds of Microsoft Office users in US-based organizations to deliver a remote access trojan (RAT) that evades detection, partially by showing up as legitimate software.

https://www.darkreading.com/threat-intelligence/phantomblu-cyberattackers-backdoor-microsoft-office-users-ole

Click above link to read more.

Back to top