August 24, 2021

Challenge yourself with our Safe Surfing quiz!

This week's stories:

Lake Cowichan RCMP phone line used to make spoof calls

The Lake Cowichan RCMP is concerned that its non-emergency phone number is being spoofed to make unsolicited calls to the public.

Since the afternoon of Tuesday, Aug. 18, the detachment has received a number of reports that people have been called from the line. Caller ID displays as Lake Cowichan RCMP, however, when the individual answers the phone, the caller hangs up. In cases where the call is missed, no message is left."

https://www.lakecowichangazette.com/news/lake-cowichan-rcmp-phone-line-used-to-make-spoof-calls/

Click above link to read more.

Back to top

T-Mobile says hack affected more than 40 million people

T-Mobile said on Tuesday that a data breach it was informed of late last week contained more than 40 million records belonging to former or prospective customers who had applied for credit with the company, as well as information on approximately 7.8 million current postpaid customer accounts.

The stolen information included first and last names, dates of birth, Social Security numbers, and driver's license information, the company said. No phone numbers, account numbers, PINs, passwords, or financial data from these accounts appeared to be taken.

https://therecord.media/t-mobile-says-hack-affected-more-than-40-million-people/

Click above link to read more.

Back to top

Iranian hackers target several Israeli organizations with supply-chain attacks

IT and communication companies in Israel were at the center of a supply chain attack campaign spearheaded by an Iranian threat actor that involved impersonating the firms and their HR personnel to target victims with fake job offers in an attempt to penetrate their computers and gain access to the company's clients.

The attacks, which occurred in two waves in May and July 2021, have been linked to a hacker group called Siamesekitten (aka Lyceum or Hexane) that has primarily singled out oil, gas, and telecom providers in the Middle East and in Africa at least since 2018, researchers from ClearSky said in a report published Tuesday.

https://thehackernews.com/2021/08/iranian-hackers-target-several-israeli.html

Click above link to read more.

Back to top

More than 600K patients affected in UNM Health hack

The University of New Mexico Health System began notifying patients earlier this month about a recent cybersecurity incident resulting in potential data exposure.

According to the system's report to the U.S. Department of Health and Human Services Office of Civil Rights, 637,252 individuals were affected.

UNM Health said that on May 2, an unauthorized third party gained access to its network and could have accessed or obtained certain files. The health system discovered the breach on June 4, more than a month later.

https://www.healthcareitnews.com/news/more-600k-patients-affected-unm-health-hack

Click above link to read more.

Back to top

Postmortem on U.S. Census hack exposes cybersecurity failures

Threat actors exploited an unpatched Citrix flaw to breach the network of the U.S. Census Bureau in January in an attack that was ultimately halted before a backdoor could be installed or sensitive data could be stolen, according to a report by a government watchdog organization.

However, investigators found that officials were informed of the flaw in its servers and had at least two opportunities to fix it before the attack, mainly due to lack of coordination between teams responsible for different security tasks, according to the report, published Tuesday by the U.S. Department of Commerce Office of Inspector General. The bureau also lagged in its discovery and reporting of the attack after it happened.

https://threatpost.com/postmortem-on-u-s-census-hack-exposes-cybersecurity-failures/168814/

Click above link to read more.

Back to top

Why phone scams are so difficult to tackle

Many of us now refuse to answer telephone calls from an unknown number, for fear that it could be a scam.

And we dread receiving a text message, purportedly from our bank or a delivery firm, again due to concerns that it might be from fraudsters.

A recent report suggests that we are right to be cautious. In the 12 months to March 2021, phone call and text message fraud across England, Wales and Northern Ireland was up 83% from the previous year, according to consumer group Which?.

https://www.bbc.com/news/business-58254354

Click above link to read more.

Back to top

Researchers detail modus operandi of ShinyHunters cyber crime group

ShinyHunters, a notorious cybercriminal underground group that's been on a data breach spree since last year, has been observed searching companies' GitHub repository source code for vulnerabilities that can be abused to stage larger scale attacks, an analysis of the hackers' modus operandi has revealed.

"Primarily operating on Raid Forums, the collective's moniker and motivation can partly be derived from their avatar on social media and other forums: a shiny Umbreon Pokémon," Intel 471 researchers said in a report shared with The Hacker News. "As Pokémon players hunt and collect "shiny" characters in the game, ShinyHunters collects and resells user data."

https://thehackernews.com/2021/08/researchers-detail-modus-operandi-of.html

Click above link to read more.

Back to top

Ransomware attack on Georgia health system endangers info of 1.4M patients

A ransomware attack discovered by St. Joseph's/Candler earlier this summer has compromised the records of 1.4 million patients.

The Savannah, Georgia-based health system published a notice this month about the incident, which took its network offline for multiple days.

"Through SJ/C's investigation it was determined that the incident resulted in an unauthorized party gaining access to SJ/C's IT network between the dates of December 18, 2020 and June 17, 2021," said the organization on its website.

"While in our IT network, the unauthorized party launched a ransomware attack that made files on our systems inaccessible," the notice continued.

https://www.healthcareitnews.com/news/ransomware-attack-georgia-health-system-endangers-info-14m-patients

Click above link to read more.

Back to top

38M records exposed via Microsoft Power Apps misconfiguration

Researchers have notified 47 public and private organizations of data exposure from Power Apps configured to allow public access.

The UpGuard research team has disclosed multiple data leaks stemming from Microsoft Power App portals configured to allow public access. A total of 38 million records have been exposed.

https://www.darkreading.com/application-security/38m-records-exposed-via-microsoft-power-apps-misconfiguration

Click above link to read more.

Back to top

Sensors and AI to monitor Dorset social care patients

One hundred people in Dorset who need social care are to be monitored by artificial intelligence (AI) as part of a three-month pilot.

Sensors installed in homes will track behaviour and electricity usage which the AI will analyse to spot potential health problems.

Lilli, the UK-based firm behind the technology, says it could cut costs and the number of care visits required.

https://www.bbc.com/news/technology-58317106

Click above link to read more.

Back to top

Waiting for a package? Don't click this phony UPS email

A clever crook has been dropping malware on unsuspecting victims who get tricked into clicking a legitimate-looking UPS tracking-number link that leads to the real UPS.com website.

Normally, you can avoid phishing and malware scams by checking the URL, or web address, of the site they take you to. It's usually a dead giveaway when the URL and purported site don't match.

https://www.tomsguide.com/news/ups-tracking-malware

Click above link to read more.

Back to top

That email asking for proof of vaccination might be a phishing scam

When people are scared, they're more likely to make mistakes. Cybercriminals take advantage of that.

As coronavirus cases rise because of the new delta variant, pandemic-related email scams are on the rise, too.

Pandemic-related phishing attempts in June increased 33 percent, compared to a lull this spring and early summer when concerns about the virus temporarily waned, researchers at security firm Proofpoint found. The spike occurred right when Google searches for "delta variant" were peaking. And as confusion about proof of vaccination and booster shots abounds, this type of attack will evolve to reflect new coronavirus concerns.

https://www.washingtonpost.com/technology/2021/08/24/covid-vaccine-proof-scam-email/

Click above link to read more.

Back to top