January 19th, 2021

Try our January "Resolutions" Quiz

This week's stories:

- More COVID scams, reporter tricked by phony Harvard job offer, and Uber wins and Twitter loses in Canadian courts
- SolarWinds hack is quickly reshaping Congress's cybersecurity agenda
- OpenWRT reports data breach after hacker gained access to forum admin account
- 'Human error' blamed for wiping hundreds of thousands of police records
- Scottish Environment Protection Agency refuses to pay ransomware crooks over 1.2GB of stolen data
- US government warns of cyberattacks targeting cloud services
- 2021 Cybersecurity Predictions

More COVID scams, reporter tricked by phony Harvard job offer, and Uber wins and Twitter loses in Canadian courts

https://www.itworldcanada.com/article/cyber-security-today-more-covid-scams-reporter-tricked-by-phony-harvard-job-offer-and-uber-wins-and-twitter-loses-in-canadian-courts/440948

More COVID-19 related scams pop up every day. But not all of them directly involve the vaccine or health products. Cybersecurity provider Proofpoint has collected a few of the most recent ones, which are often aimed at executives. Here's some of them: One claims that the world economy is approaching a turning point because of vaccines So you're invited to make some money by investing in the purchase of a troubled foreign company. Thousand of emails like that went out looking for interest in phony mergers or acquisitions. Another email campaign this month looking for phone numbers was simpler and might look like it came from an official at your firm. It says, "Would it be possible for you to complete a task for me? Before I leave for a COVID-19 meeting please give me your personal phone number."

Click link above to read more

SolarWinds hack is quickly reshaping Congress's cybersecurity agenda

https://www.csoonline.com/article/3603519/solarwinds-hack-is-quickly-reshaping-congress-s-cybersecurity-agenda.html

The federal government and private sector are still reeling from the SolarWinds supply chain hack, and Congress is on edge as it begins a new term beset by fears of domestic terrorism. It would seem all bets are off in terms of the previous legislative agenda for cybersecurity, at least in the near-term. The relevant committees in the new 117th Congress have yet to weigh in on specific pieces of legislation, but it's clear that cybersecurity will be a big focus across both the House and Senate.

Click link above to read more

OpenWRT reports data breach after hacker gained access to forum admin account

https://www.zdnet.com/article/openwrt-reports-data-breach-after-hacker-gained-access-to-forum-admin-account/

The maintainers of OpenWRT, an open-source project that provides free and customizable firmware for home routers, have disclosed a security breach that took place over the weekend.

According to a message posted on the project's forum and distributed via multiple Linux and FOSS-themed mailing lists, the security breach took place on Saturday, January 16, around 16:00 GMT, after a hacker accessed the account of a forum administrator.

"It is not known how the account was accessed: the account had a good password, but did not have two-factor authentication enabled," the message reads.

Click link above to read more

'Human error' blamed for wiping hundreds of thousands of police records

https://www.express.co.uk/news/uk/1384802/human-error-police-records-dna-Police-National-Computer-kit-malthouse-blunder-ont

Kit Malthouse said the blunder happened during routine maintenance of the Police National Computer (PNC) earlier this week, causing huge swathes of information on suspects released without further action to be lost. Officers are working "at pace" to recover the data and the incident is not thought to have put public safety at risk, according to an initial assessment.

Initially some 150,000 records were said to have been lost, but it has emerged the number is far higher than first thought at around 400,000.

Speaking to reporters on Friday, Home Office minister Mr Malthouse said the PNC was a large database of information that requires maintenance, adding: "Unfortunately down to human error, some defective code was introduced as part of that routine maintenance earlier this week and that's resulted in a deletion of some records and that's currently under investigation.

Click link above to read more

Scottish Environment Protection Agency refuses to pay ransomware crooks over 1.2GB of stolen data

https://www.theregister.com/2021/01/18/scottish_environment_protection_agency_refuses_to_pay_ransom/

Scotland's environmental watchdog has confirmed it is dealing with an "ongoing ransomware attack" likely masterminded by international "serious and organised" criminals during the last week of 2020.

"On Christmas Eve, the Scottish Environmental Protection Agency (SEPA) confirmed that it was responding to a significant cyber-attack affecting its contact centre, internal systems, processes and internal communications," it revealed.

Click link above to read more

US government warns of cyberattacks targeting cloud services

https://www.techrepublic.com/article/us-government-warns-of-cyberattacks-targeting-cloud-services/?ftag=TREa988f1c&bhid=19662319145962710268575546540229&mid=13239619&cid=712327807

Such attacks often occur when employees work remotely and use a mixture of personal and business devices to access cloud services.

Organizations with remote workers who use cloud-based services are being warned of several recent successful cyberattacks against those services.

In an advisory issued on Wednesday, CISA (Cybersecurity and Infrastructure Security Agency) revealed that hackers have been employing successful phishing campaigns, brute force login attempts, and potentially pass-the-cookie attacks to exploit weaknesses in cloud security practices. In a pass-the-cookie attack, hackers steal cookies from a user's browsing session so they can then access a certain site as the victim.

Click link above to read more

2021 Cybersecurity Predictions

https://www.itworldcanada.com/article/cyber-security-today-more-covid-scams-reporter-tricked-by-phony-harvard-job-offer-and-uber-wins-and-twitter-loses-in-canadian-courts/440948

2020 has made cybersecurity among the priorities of most organizations. The challenging times brought by the COVID pandemic showed that no corporation is immune to cyber attacks. Even the largest and seemingly secure companies suffered vulnerabilities and security lapses as they tried to adopt various communication and collaboration solutions to stay connected during the early months of remote work.

Since returning to full-time physical office operations seems unlikely, most organizations have decided to transition to hybrid and work-from-home working models permanently. That said, companies looking to navigate the new working landscape should consider the following major cybersecurity trends and predictions.

Click link above to read more