August 20th, 2019

Try our August quiz – Security While Traveling

This week's stories:

- **Saskatoon stung by $1M scam job**
- **Ransomware strike takes down 23 Texas local government agencies**
- **$11M Email Scam at Caterpillar Pinned to Nigerian Businessman**
- **Decade-Long Bank Account Hacking Scheme Gets Fraudster 57 Months**
- **Microsoft Voicemail Notifications Used As Bait in Phishing Campaign**
- **Webmin users urged to install latest version to plug vulnerability**
- **TRUMP'S CYBER CZAR IS BACK—AND HE WANTS TO MAKE HACKERS SUFFER**
- **Facebook and Twitter Scuttle Hong Kong Disinformation**
- **Biometric Security Vendor Exposes Fingerprints, Face Data**

Saskatoon stung by $1M scam job

https://www.itworldcanada.com/article/saskatoon-stung-by-1m-scam-job/420950

The finance department of every organization in the world — commercial, non-profit, government — must have business rules for dealing with partners who ask for changes in bank deposit or transfer procedures.

That's the lesson from several years of organizations being victimized by what is formally known as business email compromise fraud, where a criminal tricks managers into sending a regular payment to a different bank account. The money then disappears.

Click link above to read more

Ransomware strike takes down 23 Texas local government agencies

https://arstechnica.com/information-technology/2019/08/ransomware-strike-takes-down-23-texas-local-government-agencies/

Early on August 16, a total of 23 local government organizations in Texas were hit by a coordinated ransomware attack. The type of ransomware has not been revealed, and Texas officials asserted that no state networks were compromised in the attack.

Click link above to read more

$11M Email Scam at Caterpillar Pinned to Nigerian Businessman

https://www.bleepingcomputer.com/news/security/11m-email-scam-at-caterpillar-pinned-to-nigerian-businessman/

A Nigerian national that was on Forbes' list of the most promising entrepreneurs in Africa stands accused of business email compromise fraud that stole $11 million from one victim alone.

Obinwanne Okeke is the founder of Invictus Group, involved in construction, agriculture, oil and gas, telecoms and real estate, according. In 2016, Forbes added him to its "Africa's 30 under 30" young business owners.

Click link above to read more

Decade-Long Bank Account Hacking Scheme Gets Fraudster 57 Months

https://www.bleepingcomputer.com/news/security/decade-long-bank-account-hacking-scheme-gets-fraudster-57-months/

Brooklyn man Jason Mickel Elcock was sentenced today to 57 months in prison for a series of account hijacking attacks spanning more than a decade, having used stolen personal and financial information to pilfer over $1.1 million from banks and online retailers.

Account hijacking is a well-known tactic in identity theft schemes through which attackers profit from their victim's stolen account information to conduct unauthorized activities.

Click link above to read more

Microsoft Voicemail Notifications Used As Bait in Phishing Campaign

https://www.bleepingcomputer.com/news/security/microsoft-voicemail-notifications-used-as-bait-in-phishing-campaign/

A newly spotted phishing campaign uses Microsoft voicemail notifications as baits to trick targets into opening HTML attachments that redirect to the attackers' landing pages using a meta element.

Phishing is a type of scam where crooks try to trick their targets to provide personal info via fraudulent websites they control, using a wide range of social engineering techniques as well as messages designed to look like they're sent by a legitimate organization or someone they know.

Click link above to read more

Webmin users urged to install latest version to plug vulnerability

https://www.itworldcanada.com/article/webmin-users-urged-to-install-latest-version-to-plug-vulnerability/420987

Administrators using the open-source Webmin interface for managing Unix and Linux servers are being urged to update to the latest version after the discovery of a critical vulnerability.

The safe version is 1.930. In addition to releasing an updated version of Webmin, project developers also released Usermin 1.780.

Finding the bug, a remote code execution vulnerability (CVE-2019-15107) in the way expired passwords are handled, isn’t the big news: The big news is the hole was created by an attacker over a year ago who inserted a backdoor into the developer’s code. It remained for 1.882 through 1.921.

Click link above to read more

TRUMP'S CYBER CZAR IS BACK—AND HE WANTS TO MAKE HACKERS SUFFER

https://www.wired.com/story/tom-bossert-trinity-active-threat-interference/

Not long before Tom Bossert was pushed out of his role last year as the White House's top cybersecurity official, a public remark he made at the World Economic Forum in Davos, Switzerland, raised eyebrows.

Bossert wanted, he said, to introduce policies that would let the US government "get our hands around the necks" of the enemy hackers who cost the US billions of dollars every year. Reporters, and some fellow officials, took the comment a little too literally; after the talk, Bossert found himself explaining that he didn't mean actual, physical violence.

Click link above to read more

Facebook and Twitter Scuttle Hong Kong Disinformation

https://www.databreachtoday.com/facebook-twitter-scuttle-hong-kong-disinformation-a-12934

Social media giants Facebook and Twitter have suspended a number of accounts that they have tied to a state-backed operation meant to discredit pro-democracy protesters in Hong Kong.

Both firms as well as outside experts say there is extensive evidence tying the Chinese government to these information operations, which used fake accounts to post about local political issues, including the ongoing protests in Hong Kong, which is one of the world's leading financial centers.

Click link above to read more

Biometric Security Vendor Exposes Fingerprints, Face Data

https://www.databreachtoday.com/biometric-security-vendor-exposes-fingerprints-face-data-a-12918

A South Korean company that makes a biometric access control platform exposed fingerprint records, facial recognition data and personal information after failing to secure an Elasticsearch database, security researchers say.

Suprema, which develops an access control platform called BioStar 2, left 23GB of data, including 27.8 million records, open on the internet, according to vpnMentor, a VPN reviews website. The platform can be used to manage access to doors and elevators using devices such as smart cards and fingerprint readers.

Click link above to read more

Click Unsubscribe to stop receiving the Digest.

****

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity of each article and to apply their own judgment when using or referring to this information. The ISB is not responsible for the manner in which the information presented is used or interpreted by its recipients.

For previous issues of Security News Digest, visit the current month archive page at:

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:

Information Security Awareness Team - Information Security Branch

Office of the Chief Information Officer,

Ministry of Citizens' Services

4000 Seymour Place, Victoria, BC V8X 4S8

https:www.gov.bc.ca/informationsecurity

OCIOSecurity@gov.bc.ca

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.