



March 3rd, 2020

Try our March Quiz – [Protecting Mobile Devices](#)

This week's stories:

- [Canadians lax on checking personal data security, agency warns](#) 
- [Diabetes DIY: why thousands of people are hacking their insulin pumps](#) 
- [FCC Proposes to Fine Wireless Carriers \\$200M for Selling Customer Location Data](#)
- [Munson Healthcare hack goes undetected for nearly 3 months](#)
- [Cybercriminals are now using COVID-19 as a scam tactic](#)
- [A Flaw in Billions of Wi-Fi Chips Let Attackers Decrypt Data](#)
- [Don't be like Bezos: How to keep your phone from being hacked](#)
- [Facebook sues SDK maker for secretly harvesting user data](#)

Canadians lax on checking personal data security, agency warns 

<https://www.burnabynow.com/canadians-lax-on-checking-personal-data-security-agency-warns-1.24088521/>

Canadians are feeling less vulnerable to identity theft and are becoming lax in checking credit reports to help detect fraud, one Canada's leading credit-checking agencies says.

Global giant Equifax said Monday that 29% of recent survey respondents checked their credit report as a way of protecting their personal data over the last 12 months. And, only 38% indicated they would report fraud to a credit bureau.

[Click link above to read more](#)

Diabetes DIY: why thousands of people are hacking their insulin pumps

<https://globalnews.ca/news/6517053/diabetes-hack-insulin-pumps-health-tech/>

Thousands of people around the world with Type 1 diabetes are hacking into their medical equipment with instructions they found online. Some say it's giving them a peace of mind they never had before.

Edmonton's Jonathan Garfinkel started "looping," as it's called, about two years ago after meeting other "loopers."

Despite having no background in computer science, the writer and humanities PhD student managed to create an automated system to control his blood sugar levels.

[Click link above to read more](#)

FCC Proposes to Fine Wireless Carriers \$200M for Selling Customer Location Data

<https://krebsonsecurity.com/2020/02/fcc-proposes-to-fine-wireless-carriers-200m-for-selling-customer-location-data>

The U.S. Federal Communications Commission (FCC) today proposed fines of more than \$200 million against the nation's four largest wireless carriers for selling access to their customers' location information without taking adequate precautions to prevent unauthorized access to that data.

While the fines would be among the largest the FCC has ever levied, critics say the penalties don't go far enough to deter wireless carriers from continuing to sell customer location data.

[Click link above to read more](#)

Munson Healthcare hack goes undetected for nearly 3 months

<http://www.digitaljournal.com/tech-and-science/technology/munson-healthcare-hack-goes-undetected-for-nearly-3-months/article/568069>

Michigan-based Munson Healthcare has revealed that a hacker had lurked in their systems for over two months undetected, compromising the health and financial information of some patients. Piyush Pandey provides commentary.

Munson Healthcare group, based in northern-Michigan, found that a number of employee email accounts had been hacked. Furthermore, the accessing of the accounts had been taking place across a period of for two and a half months. The issue led to personal healthcare related information being exposed (such as patent names, dates of birth, insurance information, together with medical information).

[Click link above to read more](#)

Cybercriminals are now using COVID-19 as a scam tactic

<https://www.ctvnews.ca/health/cybercriminals-are-now-using-covid-19-as-a-scam-tactic-1.4835701>

As cases of the novel coronavirus spread around the world, scammers are attempting to profit off of concerns and paranoia by posing as health officials in online scams.

On Saturday, the World Health Organization (WHO) warned that cybercriminals are disguising themselves as WHO representatives in an effort to steal money and personal information from individuals and organizations.

These types of malicious emails, commonly referred to as phishing scams, may appear to come from the WHO and ask for sensitive information, such as usernames or passwords, or ask users to click on suspicious links or open malicious attachments. clients.

[Click link above to read more](#)

A Flaw in Billions of Wi-Fi Chips Let Attackers Decrypt Data

<https://www.wired.com/story/a-flaw-in-billions-of-wi-fi-chips-let-attackers-decrypt-data/>

Billions of devices—many of them already patched—are affected by a Wi-Fi vulnerability that allows nearby attackers to decrypt sensitive data sent over the air, researchers said on Wednesday at the RSA security conference.

The vulnerability exists in Wi-Fi chips made by Cypress Semiconductor and Broadcom, the latter a chipmaker Cypress acquired in 2016. The affected devices include iPhones, iPads, Macs, Amazon Echos and Kindles, Android devices, and Wi-Fi routers from Asus and Huawei, as well as the Raspberry Pi 3. Eset, the security company that discovered the vulnerability, said the flaw primarily affects Cypress' and Broadcom's FullMAC WLAN chips, which are used in billions of devices. Eset has named the vulnerability Kr00k, and it is tracked as CVE-2019-15126.

[Click link above to read more](#)

Don't be like Bezos: How to keep your phone from being hacked

<https://www.techrepublic.com/article/dont-be-like-bezos-how-to-keep-your-phone-from-being-hacked/>

In January, the world was surprised when the news broke that Amazon CEO Jeff Bezos had his phone hacked by the Crown Prince of Saudi Arabia, Mohammed bin Salman. But people are still buzzing about it because the idea that a corporate executive would be the target of a government is a perfectly legitimate, albeit shocking concept

[Click link above to read more](#)

Facebook sues SDK maker for secretly harvesting user data

<https://www.zdnet.com/article/facebook-sues-sdk-maker-for-secretly-harvesting-user-data/>

Facebook filed today a federal lawsuit in a California court against OneAudience, a New Jersey-based data analytics firm.

The social networking giant claims that OneAudience paid app developers to install its Software Development Kit (SDK) in their apps, and later used the control it had over the SDK's code to harvest data on Facebook users.

According to court documents obtained by ZDNet, the SDK was embedded in shopping, gaming, and utility-type apps, some of which were made available through the official Google Play Store.

[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.

