Security Digest
Information Security Branch
British Columbia
OCIO
Office of the Chief Information Officer

# February 19th, 2019

February is Cyberbullying Month

## This week's stories:

- **Canadian infosec market: Good for job seekers, 'challenging' for employers** 🇨🇦
- **U.K. report hammers Facebook, calls for tougher regulation of tech companies**
- **U.K. believes it can manage Huawei 5G risk: News report**
- **TLS 1.3 vulnerability enables hackers to eavesdrop on encrypted traffic**
- **Apple and Google urged to remove Saudi app that tracks women**
- **Elon Musk's AI writes fake news story after being given a few words**
- **Germany sees big rise in security problems affecting infrastructure**
- **WhatsApp users warned to change voicemail PINS**
- **Ukraine Announces Joint Exercises with EU to Fend Off Russian Cyber Threats**
- **Hackers Use Compromised Banks as Starting Points for Phishing Attacks**

---

### Canadian infosec market: Good for job seekers, 'challenging' for employers 🇨🇦

https://www.itworldcanada.com/article/canadian-infosec-market-good-for-job-seekers-challenging-for-employers/415097

Harry Benz knows how competitive the Canadian job market is for infosec pros. The head of a Toronto-based recruitment firm that bears his name which specializes in placing cyber security leaders has a simple tale that explains the situation:

"I got a company I deal with: For a junior person, entry level they're taking six weeks to interview. Nobody can make a decision. They're going to lose people.

"Tomorrow [Friday] I'm taking an individual who is on a work permit downtown where he's going to meet all four decision makers in one afternoon. And by Monday they'll have a decision.

**Click link above to read more**

---

### U.K. report hammers Facebook, calls for tougher regulation of tech companies

https://www.itworldcanada.com/article/u-k-report-hammers-facebook-calls-for-tougher-regulation-of-tech-companies/415116

After an 18 month investigation, British lawmakers have called for more regulation over big technology companies for failing to protect and allowing the manipulation of personal data of users, as well as facilitating the distribution of fake news.

In its final report into disinformation issued Monday, the House of Commons digital, culture and media committee said "companies like Facebook should not be allowed to behave like 'digital gangsters' in the online world, considering themselves to be ahead of and beyond the law."

**Click link above to read more**

---

### U.K. believes it can manage Huawei 5G risk: News report

https://www.itworldcanada.com/article/u-k-believes-it-can-manage-huawei-5g-risk-news-report/415123

The British government may have found a way out of increasing pressure to ban equipment from Huawei Technologies from being used in the new 5G cellular networks because of concerns the company will crumble under pressure from China to help in spying on commercial companies and governments.

According to Reuters and the Financial Review, the U.K. National Cyber Security Centre has determined that there are ways to limit the risks from using Huawei gear.

**Click link above to read more**

---

### TLS 1.3 vulnerability enables hackers to eavesdrop on encrypted traffic

https://www.scmagazineuk.com/tls-13-vulnerability-enables-hackers-eavesdrop-encrypted-traffic/article/1525916?bulletin=sc-newswire

Academics have found a vulnerability in TLS1.3 which allows hackers to intercept encrypted traffic to steal data which was thought to be safe and secure.

According to a research paper published by academics at Tel Aviv University, University of Adelaide, University of Michigan and the Weizmann Institute, as well as the NCC Group and Data61, the latest attack is a variation of the original Bleichenbacher oracle attack that was able to decrypt an RSA encrypted message using the Public-Key Cryptography Standards.

**Click link above to read more**

---

### Apple and Google urged to remove Saudi app that tracks women

https://www.cnn.com/2019/02/13/tech/saudi-app-absher-google-apple-intl/index.html

Human rights defenders are calling on Apple (AAPL) and Google (GOOGL) to remove the Saudi government app Absher from its platforms, saying that it allows Saudi men to track women under their sponsorship.

In a letter addressed to Apple's CEO Tim Cook and Google's CEO Sundar Pichai Monday, the top Democrat on the US Senate Finance Committee, Sen. Ron Wyden of Oregon, asked the tech giants to prevent their technical infrastructure and app stores from being used for enabling "abhorrent surveillance and control of women."

**Click link above to read more**

---

### Elon Musk's AI writes fake news story after being given a few words

https://www.stuff.co.nz/technology/digital-living/110634967/elon-musks-ai-writes-fake-news-story-after-being-given-a-few-words

OpenAI, an artificial intelligence research group co-founded by billionaire Elon Musk, has demonstrated a piece of software that can produce authentic-looking fake news articles after being given just a few pieces of information.

In an example published Thursday by OpenAI, the system was given some sample text: "A train carriage containing controlled nuclear materials was stolen in Cincinnati today. Its whereabouts are unknown."

**Click link above to read more**

---

### Germany sees big rise in security problems affecting infrastructure

https://news.hitb.org/content/germany-sees-big-rise-security-problems-affecting-infrastructure

Germany has experienced a big increase in the number of security incidents hitting critical infrastructure such as power grids and water suppliers, the BSI cybersecurity agency said on Sunday, adding however that they were not all due to hacking.

The Welt am Sonntag weekly had reported on Sunday that Germany had learned of 157 hacker attacks on critical infrastructure companies in the second half of 2018 compared to 145 attacks in the whole of the previous year.

“The number of reports of IT security incidents has increased but it is not to be equated with the number of cyber attacks,” tweeted the BSI in response to the newspaper report.

**Click link above to read more**

## WhatsApp users warned to change voicemail PINS

https://news.hitb.org/content/whatsapp-users-warned-change-voicemail-pins

Australia’s Stay Smart Online is warning WhatsApp users to change their mobile’s voicemail PIN from the default PIN, if they haven’t done so already.

Attackers are allegedly gaining access to users’ WhatsApp accounts by using the default voicemail PIN to access voice authentication codes. Those codes can allow the attacker to use a victim’s WhatsApp account on the attacker’s own device.

The attack method isn’t new – it has been doing the rounds since 2017 and Israel’s National Cyber Directorate issued a warning about it - however people are still falling victim to the attack.

**Click link above to read more**

## Ukraine Announces Joint Exercises with EU to Fend Off Russian Cyber Threats

https://www.bleepingcomputer.com/news/security/ukraine-announces-joint-exercises-with-eu-to-fend-off-russian-cyber-threats/

According to a statement made by the Secretary of the National Security and Defense Council of Ukraine Oleksandr Turchinov, Ukraine will organize a number of joint exercises in the near future with the European Union (EU) designed to develop appropriate response models to Russian cyber threats.

Turchinov said that having a set of responses ready for various cyber attacks scenarios would allow the country to better counteract cyberspace aggression and avoid Russian interference during future presidential elections in Ukraine.

**Click link above to read more**

## Hackers Use Compromised Banks as Starting Points for Phishing Attacks

https://www.bleepingcomputer.com/news/security/hackers-use-compromised-banks-as-starting-points-for-phishing-attacks/

Cybercriminals attacking banks and financial organizations use their foothold in a compromised infrastructure to gain access to similar targets in other regions or countries.

In a report released today and shared with BleepingComputer, international security company Group-IB specialized in preventing cyber attacks describes a so called cross-border domino-effect that can lead to spreading an infection beyond the initial target. The report is based on information from incident response work conducted in 2018 by the company's team of computer forensics experts.

**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.

Information Security Branch
www.gov.bc.ca/informationsecurity

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer