



## October 1<sup>st</sup>, 2018

October is "[Cybersecurity awareness](#)" Month

Test yourself with the Cybersecurity Awareness Month Quiz: [Cybersecurity by the Numbers](#)

### This week's stories:

- [Cyber Security Awareness Month: Canadian firms not training enough, says expert](#) 
- [Sting operation uncovers 'dark web' fentanyl dealer in Kelowna](#) 
- [90 million Facebook users have to log back in after security incident](#)
- [Honour of Kings \(video game\) uses facial recognition to check ages](#)
- [Tesco Bank fined £16.4m over cyber-attack](#)
- [Conservative Party conference app reveals MPs' numbers](#)
- [Sites Trick Users Into Subscribing to Browser Notification Spam](#)
- [Port of San Diego Affected by a Ransomware Attack](#)
- [2 men arrested in Oklahoma, suspected in \\$14 million cryptocurrency theft, hacking of California company](#)
- [FDA Reveals Steps to Bolster Medical Device Cybersecurity](#)
- [Malware steals passwords from 6.4 million SHEIN customers](#)
- [Air Miles on Sale on the Dark Web at a Fraction of the Cost](#)
- [UK's MI5 just admitted to unlawful spying on citizens and their whereabouts](#)

---

### **Cyber Security Awareness Month: Canadian firms not training enough, says expert**

<https://www.itworldcanada.com/article/cyber-security-awareness-month-canadian-firms-not-training-enough-says-expert/409462>

Oops! That's the word infosec pros don't want to hear from an organization's staff. But after years of warnings, pleas, posters, online training, video training and email reminders, they're hearing it more often than ever.

Employees are still clicking where they shouldn't, using unsafe passwords, re-using passwords or uploading sensitive data to cloud storage sites.

And if that isn't enough sometimes IT staff who should know better wrongly configure something.

[Click link above to read more](#)

---

## Sting operation uncovers 'dark web' fentanyl dealer in Kelowna

<https://globalnews.ca/news/4494195/kelowna-fentanyl-dealer/>

His name was Robert Kiessling: a 40-year-old instructor at Okanagan College who was living a double life as a drug dealer. Kiessling was not your average street dealer; he was dealing fentanyl over the dark web.

His handle on the dark web was DougFish44, or DF44. In September 2017, the RCMP tipped off American law officials about his suspicious activity.

[Click link above to read more](#)

---

## 90 million Facebook users have to log back in after security incident

<https://www.itworldcanada.com/article/90-million-facebook-users-have-to-log-back-in-after-security-incident/409422>

It's not been a good week for Facebook.

Today the social media giant admitted almost 50 million accounts may have been compromised by an unknown attacker who got access to security tokens used so they don't have to re-enter passwords every time they use the service, with another 40 million under question. As a result, 90 million subscribers have been kicked off and asked to login again after the company changed access tokens.

It may also affect other web sites where people use their Facebook credentials for logging in.

[Click link above to read more](#)

---

## Honour of Kings uses facial recognition to check ages

<https://www.bbc.com/news/technology-45707469>

Honour of King's publisher Tencent announced the move at the weekend.

It said the trial would initially be limited to "thousands" of new players based in Beijing and Shenzhen.

The title has been criticised in local media over claims children have become addicted to it. But one expert questioned whether the test could be scaled up.

The mobile app resembles League of Legends and pits players against each other in multiplayer online battles set in a fantasy world.

[Click link above to read more](#)

---

## Tesco Bank fined £16.4m over cyber-attack

<https://www.bbc.com/news/business-45704273>

Tesco Bank has been fined £16.4m by the UK financial regulator for failings surrounding a cyber-attack on its customers in November 2016.

The Financial Conduct Authority said the bank had failed to exercise due skill, care and diligence in protecting its personal current account holders.

The fraudsters got away with £2.26m. Tesco Bank said all the money had been refunded to account holders.

It added it was "very sorry" for the impact the attack had had on customers.

[Click link above to read more](#)

---

## Conservative Party conference app reveals MPs' numbers

<https://www.bbc.com/news/uk-politics-45693143>

Conservative MPs including Boris Johnson have had their phone numbers and other personal details revealed by the party's conference app.

A Guardian columnist highlighted the security breach on Twitter and the BBC was also able to access private details of people attending the event.

The Conservative Party apologised for "any concern caused" and said "the technical issue has been resolved".

The Information Commissioner's Office said it would be making inquiries.

BBC political correspondent Chris Mason said the technical glitch was "deeply, deeply embarrassing" for the party.

[Click link above to read more](#)

---

## Sites Trick Users Into Subscribing to Browser Notification Spam

<https://www.bleepingcomputer.com/news/security/sites-trick-users-into-subscribing-to-browser-notification-spam/>

Sites that try to trick users into subscribing to browser notification spam are increasingly becoming a method used to promote unwanted extensions, fake software, adware bundles, adult sites, and scam sites.

[Click link above to read more](#)

---

## Port of San Diego Affected by a Ransomware Attack

<https://www.bleepingcomputer.com/news/security/port-of-san-diego-affected-by-a-ransomware-attack/>

On September 25th, the Port of San Diego announced that their information technology systems had been disrupted by a cyber attack. In an announcement today, it was announced that this disruption was caused by a ransomware attack.

[Click link above to read more](#)

---

## 2 men arrested in Oklahoma, suspected in \$14 million cryptocurrency theft, hacking of California company

<https://kfor.com/2018/09/28/2-men-arrested-in-oklahoma-suspected-in-14-million-cryptocurrency-theft-hacking-of-california-company/>

OKLAHOMA CITY – Two men arrested in Oklahoma City this week are suspected of hacking and stealing millions of dollars from a California-based cryptocurrency company.

Fletcher Robert Childers, 23, and Joseph Harris, 21, both of Missouri, were arrested by Oklahoma City Police at a west side hotel Monday. According to court documents, the two are suspects in a \$14 million theft from Crowd Machine, headquartered in San Jose.

[Click link above to read more](#)

---

## FDA Reveals Steps to Bolster Medical Device Cybersecurity

<https://www.databreachtoday.com/fda-reveals-steps-to-bolster-medical-device-cybersecurity-a-11575>

In its ongoing quest to improve the state of medical device cybersecurity, the Food and Drug Administration has announced a number of key moves - including the release of a new security playbook,

plans to leverage information sharing and analysis organizations, and an effort to update its 2014 premarket guidance for manufacturers.

[Click link above to read more](#)

---

### Malware steals passwords from 6.4 million SHEIN customers

<https://hotforsecurity.bitdefender.com/blog/malware-steals-passwords-from-6-4-million-shein-customers-20375.html>

Women's fashion retailer SHEIN has suffered a major security breach that has exposed the personal information and passwords of over six million customers.

In a press statement, SHEIN reveals that it discovered on August 22 2018 that malicious hackers had compromised its computer network, and that between June and early August 2018 customer email addresses and "encrypted password credentials" had been stolen.

[Click link above to read more](#)

---

### Air Miles on Sale on the Dark Web at a Fraction of the Cost

<https://hotforsecurity.bitdefender.com/blog/air-miles-on-sale-on-the-dark-web-at-a-fraction-of-the-cost-20368.html>

If you want a discount on your next flight or hotel reservation, or maybe an upgrade to business class, you might try looking in unexpected places. Who would have thought frequent flyer miles could be purchased on the Dark Web?

There's a first time for everything and, yes, there is a black market for air miles – Dream Market, Olympus Market and Berlusconi Market. Aren't drugs profitable anymore? Or maybe hackers are bored and trying to expand operations. Points can be reclaimed through gift cards, and identification is rarely required, which makes it very easy for criminals to further use.

[Click link above to read more](#)

---

### UK's MI5 just admitted to unlawful spying on citizens and their whereabouts

<https://www.firstpost.com/tech/news-analysis/uks-mi5-just-admitted-to-unlawful-spying-on-citizens-and-their-whereabouts-5263751.html>

In what comes across as a shocking revelation, UK's domestic counter-intelligence and security agency, commonly referred to as the MI5, today admitted to capturing and reading private data belonging to a campaign group named Privacy International.

According to a report by Bloomberg, Judge Michael Burton said in court on Tuesday that the MI5 allegedly held and "accessed or examined" data about the organisation. However, the London judge did not elaborate on the type of data collected or why was it viewed in the first place.

[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](mailto: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.

