



**November 17<sup>th</sup>, 2020**  
Try our November - '[Phishing](#)' Quiz

**This week's stories:**

- [Cleanup from Saint John cyberattack could last months, says cyber security expert](#)
- [Canada PM refuses to commit to Huawei 5G decision timetable](#)
- [BCIT and other academic institutions join Fortinet's Security Academy Program](#)
- [Google Chrome Update Gets Serious: Homeland Security \(CISA\) Confirms Attacks Underway](#)
- [Snooping where we sleep](#)
- [How to secure your Zoom account with two-factor authentication](#)
- [The CostaRicto Campaign: Cyber-Espionage Outsourced](#)
- [Breach Lawsuit Spotlights Complex Vendor Issues](#)
- [The Hot New Covid Tech Is Wearable and Constantly Tracks You](#)
- [Scammers Expose Facebook Data Haul of 13 Million Records](#)
- [4 Phishing Scams You Need to Beware of This Holiday Season](#)

---

**Cleanup from Saint John cyberattack could last months, says cyber security expert**

<https://www.cbc.ca/news/canada/new-brunswick/cyber-security-saint-john-1.5803298>

A cyberattack on a municipality never comes at a good time, but a cyber security expert says the attack on Saint John's internet infrastructure comes at a particularly bad time.

On Sunday, the city announced there'd been a "significant" cyberattack, which forced it to shut down several online services, including payment systems, email and the city's website.

*[Click link above to read more](#)*

---

**Canada PM refuses to commit to Huawei 5G decision timetable**

<https://news.yahoo.com/canada-pm-refuses-commit-huawei-205418492.html>

Canadian Prime Minister Justin Trudeau -- under pressure from the opposition to ban Huawei from the country's 5G networks -- refused to say Tuesday when he might make his decision, or if it would come before year's end.

*[Click link above to read more](#)*

---

## **BCIT and other academic institutions join Fortinet's Security Academy Program**

<https://www.itworldcanada.com/article/bcit-and-other-academic-institutions-join-fortinets-security-academy-program/438343>

Fortinet's Security Academy Program is adding to its list of academic institutions that form the program's backbone.

The British Columbia Institute of Technology (BCIT), Seneca College of Applied Arts and Technology and the Ontario College of Management and Technology are joining Fortinet's Security Academy Program.

*[Click link above to read more](#)*

---

## **Google Chrome Update Gets Serious: Homeland Security (CISA) Confirms Attacks Underway**

<https://www.forbes.com/sites/daveywinder/2020/11/15/google-chrome-update-gets-serious-homeland-security-cisa-confirms-attacks-underway/>

Within the space of just three short weeks, Google has patched no less than five potentially dangerous vulnerabilities in the Chrome web browser.

These are not your common vulnerabilities either, but rather ones known as zero-days. A zero-day being a vulnerability that is being actively exploited by attackers while remaining unknown to the vendor or threat intelligence outfits.

*[Click link above to read more](#)*

---

## **Snooping Where We Sleep**

<https://www.stopspying.org/snooping>

Across the US, K-12 schools and universities have shifted to remote instruction to contain the spread of COVID-19. In doing so, an increasing number are using a dystopian set of surveillance tools to discourage cheating, including facial recognition to identify test-takers, video monitoring to flag supposedly suspicious behavior, and remote access to students' computers to control their activity during exams. The need for these tools is not clear: evidence suggests that students cheat less on online exams than in traditional classroom settings.

*[Click link above to read more](#)*

---

## **How to secure your Zoom account with two-factor authentication**

<https://www.techrepublic.com/article/how-to-secure-your-zoom-account-with-two-factor-authentication/>

Zoom now provides an extra level of security to your account with two-factor authentication (2FA). With Zoom's flavor of 2FA, you can verify your account through your mobile device with codes sent via SMS or from a dedicated authenticator app such as Google Authenticator. Whichever method you use, enabling

2FA can help protect your Zoom account. Let's see how this works.

[\*Click link above to read more\*](#)

---

### **The CostaRicto Campaign: Cyber-Espionage Outsourced**

<https://blogs.blackberry.com/en/2020/11/the-costaricto-campaign-cyber-espionage-outsourced>

During the past six months, the BlackBerry Research and Intelligence team have been monitoring a cyber-espionage campaign that is targeting disparate victims around the globe. The campaign, dubbed CostaRicto by BlackBerry, appears to be operated by “hackers-for-hire”, a group of APT mercenaries who possess bespoke malware tooling and complex VPN proxy and SSH tunnelling capabilities.

Mercenary groups offering APT-style attacks are becoming more and more popular. Their tactics, techniques, and procedures (TTPs) often resemble highly sophisticated state-sponsored campaigns, but the profiles and geography of their victims are far too diverse to be aligned with a single bad actor's interests.

[\*Click link above to read more\*](#)

---

### **Breach Lawsuit Spotlights Complex Vendor Issues**

<https://www.healthcareinfosecurity.com/breach-lawsuit-spotlights-complex-vendor-issues-a-15345>

A medical device maker has sued an IT vendor in the wake of an email server migration mishap that exposed the health data of more than 277,000 individuals. The case illustrates the complexities of vendor risk management - especially after mergers and acquisitions.

In its lawsuit, Zoll Medical Corp. alleges that Campbell, Calif.-based Barracuda Networks was negligent in "failing to take reasonable precautions and safeguards" to protect Zoll's data from disclosure to unauthorized third parties.

[\*Click link above to read more\*](#)

---

### **The Hot New Covid Tech Is Wearable and Constantly Tracks You**

<https://www.nytimes.com/2020/11/15/technology/virus-wearable-tracker-privacy.html>

In Rochester, Mich., Oakland University is preparing to hand out wearable devices to students that log skin temperature once a minute — or more than 1,400 times per day — in the hopes of pinpointing early signs of the coronavirus.

In Plano, Texas, employees at the headquarters of Rent-A-Center recently started wearing proximity detectors that log their close contacts with one another and can be used to alert them to possible virus exposure.

[\*Click link above to read more\*](#)

---

### **Scammers Expose Facebook Data Haul of 13 Million Records**

<https://www.infosecurity-magazine.com/news/scammers-expose-facebook-data-13/>

Security researchers have uncovered a major Facebook scam exploiting hundreds of thousands of users, after the scammers left an Elasticsearch server unsecured.

Among the 5.5GB haul discovered by vpnMentor on September 21, was 150,000-200,000 Facebook usernames and passwords, and personal info including emails, names and phone numbers for hundreds of thousands who had fallen victim to a Bitcoin scam.

[Click link above to read more](#)

---

#### 4 Phishing Scams You Need to Beware of This Holiday Season

<https://www.greathorn.com/blog-4-phishing-scams-you-need-to-beware-of-this-holiday-season/>

With the holiday season just around the corner, it appears that online retailers will be the “go to” for shoppers. Black Friday sales, digital advertising, promotional emails and mixed within these emails will be a long-time holiday staple – phishing attacks.

Cyber-attacks, using phishing, spike during the holiday season every year. It is a perfect time for cybercriminals to launch campaigns, preying on multi-tasking, stress, and urgency to get consumers to act quickly. The holiday season presents an ideal opportunity for cybercriminal to get us to fall victim to their scams.

[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:

<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.

