






May 19, 2020

Try our May Quiz – [Cyber Safety at Home](#)

Save the Date for Security Day – <http://www.gov.bc.ca/securityday>

This week's stories:

- [Fake Canada website among many using COVID-19 relief offers to phish for credentials](#) 
- [CSIS says proposed federal privacy reforms could hinder spy operations](#) 
- [Canadian small businesses receive free cybersecurity test from Mastercard](#) 
- [Tech assisted COVID-19 tracking is having some issues](#)
- [Three factors involved in the bulk of data breaches: Verizon](#)
- [Virtual Parliament struggling with technology, security, interpretation, report says](#)
- [EasyJet hacked: data breach affects 9 million customers](#)
- [Google rolls out new Enhanced Safe Browsing security feature](#)
- [Bluetooth Bugs Allow Impersonation Attacks on Legions of Devices](#)
- [WordPress Page Builder Plugin Bugs Threaten 1 Million Sites with Full Takeover](#)

Fake Canada website among many using COVID-19 relief offers to phish for credentials



<https://www.itworldcanada.com/article/fake-canada-website-among-many-using-covid-19-relief-offers-to-phish-for-credentials/430809>

With governments around the world making billions of dollars available for COVID-19 financial relief, criminals are making every effort to take advantage. That includes building phony official coronavirus relief templates for websites to trick victims into giving up sensitive personal information.

[Click link above to read more](#)

CSIS says proposed federal privacy reforms could hinder spy operations 

<https://www.canadiansecuritymag.com/csis-says-proposed-federal-privacy-reforms-could-hinder-spy-operations/>

Canada's spy agency has warned the Trudeau government that proposed changes to bolster privacy could undermine the ability of intelligence agents to collect and use information about citizens.

In a 14-page submission to the Justice Department, the Canadian Security Intelligence Service recommends any reforms include special language that takes into account "the critical public interest in national security activities" carried out by CSIS.

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

Canadian small businesses receive free cybersecurity test from Mastercard

<https://www.canadiansecuritymag.com/canadian-small-businesses-receive-free-cybersecurity-test-from-mastercard/>

TORONTO – As small businesses across Canada cope with ongoing social distancing requirements, many are quickly moving their activities online and facing greater exposure to cyber threats.

To help small businesses protect their operations, Mastercard announced that RiskRecon, a Mastercard company, is providing Canadian small businesses free cybersecurity assessments through Dec. 31, 2020.

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

Tech assisted COVID-19 tracking is having some issues

<https://www.canadiansecuritymag.com/tech-assisted-covid-19-tracking-is-having-some-issues/>

Harnessing today's technology to the task of fighting the coronavirus pandemic is turning out to be more complicated than it first appeared.

The first U.S. states that rolled out smartphone apps for tracing the contacts of COVID-19 patients are dealing with technical glitches and a general lack of interest by their residents. A second wave of tech-assisted pandemic surveillance tools is on its way, this time with the imprimatur of tech giants Apple and Google. But those face their own issues, among them potential accuracy problems and the fact that they won't share any information with governments that could help track the spread of the illness.

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

Three factors involved in the bulk of data breaches: Verizon

<https://www.itworldcanada.com/article/three-factors-involved-in-the-bulk-of-data-breaches-verizon/430915>

Credential theft, social engineering attacks (including phishing and business email compromise) and human errors were involved in just over two-thirds of almost 4,000 data breaches around the world last year, according to the 13th annual Verizon Data Breach Investigations Report.

"These tactics prove effective for attackers," say the report's authors, so they return to them time and again. For most organizations, these three tactics should be the focus of the bulk of security efforts."

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

Virtual Parliament struggling with technology, security, interpretation, report says

<https://www.cbc.ca/news/politics/ommons-virtual-parliament-vote-translation-report-1.5572951>

A House of Commons committee has made a number of recommendations it says are required to improve its work during the pandemic including becoming fully virtual, improving cyber security and dealing with a translation service that is "dangerously close" to being unable to do its job.

A report by the standing committee on procedure and House affairs released Friday, took a look at the challenges facing Parliament as it strives to continue operating despite much of the rest of the country being shut down due to the pandemic.

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

EasyJet hacked: data breach affects 9 million customers

<https://www.bleepingcomputer.com/news/security/easyjet-hacked-data-breach-affects-9-million-customers/>

EasyJet, the UK's largest airline, has disclosed that they were hacked and that the email addresses and travel information for 9 million customers were exposed. For some of these customers, credit card details were also accessed by the attackers.

In a data breach notification disclosed today, EasyJet states that they have suffered a cyberattack, and an unauthorized third-party was able to gain access to their systems.

During this attack, the threat actors were able to access the email addresses and travel information for nine million customers. For approximately 2,208 customers, credit card details were also exposed.

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

Google rolls out new Enhanced Safe Browsing security feature

<https://www.bleepingcomputer.com/news/google/google-rolls-out-new-enhanced-safe-browsing-security-feature/>

Today, Google has announced a new Enhanced Safe Browsing feature that will offer real-time protection against known malicious web sites and downloads.

Since 2007, Google has offered the Safe Browsing feature to protect users from malicious web sites and files that contain malware, display phishing pages, or attempt to install malicious files.

Since its release, numerous browsers, including Google Chrome, Firefox, and Safari, utilize this security feature to protect their users from online threats.

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

Bluetooth Bugs Allow Impersonation Attacks on Legions of Devices

<https://threatpost.com/bluetooth-bugs-impersonation-devices/155886/>

A host of unpatched security bugs that allow BIAS attacks affects Bluetooth chips from Apple, Intel, Qualcomm, Samsung and others.

Academic researchers have uncovered security vulnerabilities in Bluetooth Classic that allows attackers to spoof paired devices: They found that the bugs allow an attacker to insert a rogue device into an established Bluetooth pairing, masquerading as a trusted endpoint. This allows attackers to capture sensitive data from the other device.

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

WordPress Page Builder Plugin Bugs Threaten 1 Million Sites with Full Takeover

<https://threatpost.com/wordpress-page-builder-bugs-takeover/155659/>

Severe CSRF to XSS bugs open the door to code execution and complete website compromise.

Page Builder by SiteOrigin, a WordPress plugin with a million active installs that's used to build websites via a drag-and-drop function, harbors two flaws that can allow full site takeover.

According to researchers at WordPress, both security bugs can lead to cross-site request forgery (CSRF) and reflected cross-site scripting (XSS). They "allow attackers to forge requests on behalf of a site administrator and execute malicious code in the administrator's browser," according to Wordfence researchers, in a Monday posting.

[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

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.

