




**September 8<sup>th</sup>, 2020**  
Try our September - '[Passwords](#)' Quiz

### **This week's stories:**

- [Technical Approaches to Uncovering and Remediating Malicious Activity \(CISA\)](#) 
- [Canadian law firms team up to file class-action suit against Google](#) 
- [Algorithmic policing technology threatens Canadians' privacy, says research group](#) 
- [Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems](#)
- [Why Election Interference Attempts Are Getting Harder to Detect](#)
- [Vishing scams use Amazon and Prime as lures – don't get caught!](#)
- [Iranian Hackers Reportedly Selling Network Access to Others](#)
- [Facebook & Twitter Remove Russian Accounts Spreading Disinformation](#)
- [Cryptobugs Found in Numerous Google Play Store Apps](#)

---

### **Technical Approaches to Uncovering and Remediating Malicious Activity**

<https://us-cert.cisa.gov/ncas/alerts/aa20-245a>

#### **Summary**

This joint advisory is the result of a collaborative research effort by the cybersecurity authorities of five nations: Australia,[1] Canada,[2] New Zealand,[3][4] the United Kingdom,[5] and the United States.[6] It highlights technical approaches to uncovering malicious activity and includes mitigation steps according to best practices. The purpose of this report is to enhance incident response among partners and network administrators along with serving as a playbook for incident investigation.

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

---

### **Canadian law firms team up to file class-action suit against Google**

<https://www.itworldcanada.com/article/canadian-law-firms-team-up-to-file-class-action-suit-against-google/435459>

Lawyers in British Columbia, Ontario and Quebec have filed proposed class-action lawsuits in the three provinces against Google and its parent Alphabet Inc. on behalf of millions of Canadians, alleging the company unlawfully collects and profits from personal information without their consent.

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

---

### **Algorithmic policing technology threatens Canadians' privacy, says research group**

<https://www.itworldcanada.com/article/algorithmic-policing-technology-threatens-canadians-privacy-says-research-group/435323>

The increasing use of algorithmic surveillance technologies by Canadian police threatens privacy and fundamental freedoms, says a University of Toronto technology and rights research group.

"The advanced capabilities and heightened data requirements of algorithmic policing technologies introduce new threats to privacy," says a report issued Tuesday by Citizen Lab.

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

---

### **Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems**

<https://www.whitehouse.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/>

SUBJECT: Cybersecurity Principles for Space Systems

Section 1. Background. The United States considers unfettered freedom to operate in space vital to advancing the security, economic prosperity, and scientific knowledge of the Nation. Space systems enable key functions such as global communications; positioning, navigation, and timing; scientific observation; exploration; weather monitoring; and multiple vital national security applications. Therefore, it is essential to protect space systems from cyber incidents in order to prevent disruptions to their ability to provide reliable and efficient contributions to the operations of the Nation's critical infrastructure.

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

---

### **Why Election Interference Attempts Are Getting Harder to Detect**

<https://therecord.media/why-election-interference-attempts-are-getting-harder-to-detect/>

When Facebook disclosed earlier this week that a Kremlin-backed group was running a disinformation campaign that hired real journalists to write about domestic politics, one thing stood out: Russian threat actors targeting the election are going to much greater lengths to avoid getting caught.

Following the 2016 presidential election and 2018 midterms, which were marked by a variety of foreign efforts to influence voting behavior, cybersecurity experts and government officials have been on high alert to spot similar campaigns ahead of the upcoming election. However, the Russian threat actors that targeted previous votes have seemed to mostly remain on the sidelines, according to a report released today by Recorded Future.

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

---

### **Vishing scams use Amazon and Prime as lures – don't get caught!**

<https://nakedsecurity.sophos.com/2020/09/03/vishing-scams-use-amazon-and-prime-as-lures-dont-get-caught/>

Well-known US cybercrime journalist Brian Krebs recently published a warning about vishing attacks against business users.

The FBI promptly followed up on Krebs's article with a warning of its own, dramatically entitled Cyber criminals take advantage of increased telework through vishing campaign.

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

---

### **Iranian Hackers Reportedly Selling Network Access to Others**

<https://www.bankinfosecurity.com/iranian-hackers-reportedly-selling-network-access-to-others-a-14933>

"Pioneer Kitten," which has been in operation since 2017, has targeted numerous organizations and government agencies in the U.S., the Middle East and Israel, according to a new CrowdStrike report.

Members of the hacking group have recently started selling access to vulnerable corporate and government networks on various underground sites in an effort to generate cash for the hackers, the report states.

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

---

### **Facebook & Twitter Remove Russian Accounts Spreading Disinformation**

<https://www.darkreading.com/threat-intelligence/facebook-and-twitter-remove-russian-accounts-spreading-disinformation/d/d-id/1338825>

Facebook and Twitter have removed social media accounts linked to the Russia-backed Internet Research Agency (IRA), which has returned with new efforts to sway Americans in the 2020 presidential election using a fraudulent news website and several fake social media profiles.

The IRA is a Russian organization known for its massive operation to influence the results of the 2016 election with disinformation tactics. Researchers with Graphika who analyzed its latest activity say it's using new methods to achieve a familiar goal: to persuade voters away from the campaign of Joe Biden and Kamala Harris, similar to its efforts against Hillary Clinton in 2016

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

---

### **Cryptobugs Found in Numerous Google Play Store Apps**

<https://threatpost.com/cryptobugs-found-in-numerous-google-play-store-apps/159013/>

Researchers have discovered more than 300 apps on the Google Play Store breaking basic cryptography code using a new tool they developed to dynamically analyze it.

Academics from Columbia University developed a custom tool, CRYLOGGER, that analyzes Android applications for unsafe use of cryptographic code according to 26 basic cryptography rules. Those rules include avoiding the use of: broken hash functions, bad passwords, reusing passwords multiple times, HTTP URL connections or a "badly-derived" key for encryption.

[\*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.

