




**January 7<sup>th</sup>, 2020**

Try our January Quiz - [Resolutions](#)

Save the date - February 5<sup>th</sup> to 7<sup>th</sup> is the [Privacy and Security Conference](#)

**This week's stories:**

- [Hackers access Sask. eHealth system, demand ransom](#) 
- [Editor's picks: Most pressing cybersecurity stories in 2019](#)
- [Austria's Foreign Ministry Hit by Cyber-Attack](#)
- [The Top 10 Cybersecurity Stories Of 2019—A Window Onto The 2020 Threatscape](#)
- [Iran 'revenge' could come in the form of cyber-attacks, experts warn](#)
- [Automotive cybersecurity incidents doubled in 2019, up 605% since 2016](#)
- [Here are the top cybersecurity predictions for 2020](#)
- [Why is Brazil so vulnerable to cyber attacks?](#)
- [Widely Known Flaw in Pulse Secure VPN Being Used in Ransomware Attacks](#)
- [Malicious Google Play Apps Linked to SideWinder APT](#)
- [9 clever ways thieves steal your identity – and how you can stop them](#)
- [Before you buy anything else on Amazon, read this important warning](#)

---

**Hackers access Sask. eHealth system, demand ransom**

<https://regina.ctvnews.ca/hackers-access-sask-ehealth-system-demand-ransom-1.4755629>

REGINA -- Hackers made it through the first level of security for Saskatchewan's eHealth records system this weekend, locking the government out of some systems.

Jim Hornell with eHealth Saskatchewan told CTV News the hackers are demanding the government pay an unspecified ransom to get the system back under its control.

[Click link above to read more](#)

---

**Editor's picks: Most pressing cybersecurity stories in 2019**

<https://searchsecurity.techtarget.com/feature/Editors-picks-Most-pressing-cybersecurity-stories-in-2019>

Some of the most popular coverage on SearchSecurity in 2019 highlighted current and emerging threats to organizations across verticals, while other articles offered insights to problems that have been plaguing enterprises for years, along with their well-known and new solutions.

Check out some of the most popular articles with readers this year that dig into the threat landscape of today and tomorrow, with expert advice on how to maneuver that balance.

[Click link above to read more](#)

---

**Austria's Foreign Ministry hit by Cyber Attack**

<https://www.infosecurity-magazine.com/news/austria-foreign-ministry/>

The Austrian government has been hit by a cyber-attack that could be the work of a rival foreign power.

The attack, which was leveled against the country's Foreign Ministry, began late on Saturday night. A spokesperson for the ministry described the incident as "serious" and said that experts had warned it could continue for several days.

On the same day the attack was launched, at a congress held in the city of Salzburg, Austria's Green Party said that it was in favor of forming a coalition with the conservative People's Party.

The ministry said that the attack had been caught early and countermeasures had immediately been put in place. The signatures and the pattern of the attack suggest that it could be the work of a state-sponsored threat actor.

[Click link above to read more](#)

---

## The Top 10 Cybersecurity Stories Of 2019—A Window Onto The 2020 Threatscape

<https://www.forbes.com/sites/daveywinder/2019/12/27/the-top-10-cybersecurity-stories-of-2019-a-window-onto-the-2020-threatscape/?ss=consumertech#1e37b5c37992>

There can be no doubt, as 2019 draws ever closer to an end, that it has been quite the year as far as cybersecurity is concerned. I have reported on everything from the world's top 100 worst passwords to how Apple's iPhone FaceID was "hacked" in less than 120 seconds.

The year didn't even start on a high note, with the revelation of the "Collection 1" data dump affecting more than 770 million people. Within a month, this had been followed by collections two to five, taking the total number of hacked accounts involved to 2.2 billion. Hardly surprising, then, that the first six months of 2019 alone saw data breaches expose more than 4 billion records.

[Click link above to read more](#)

---

## Iran 'revenge' could come in the form of cyber-attacks, experts warn

<https://www.theguardian.com/world/2020/jan/03/iran-cyberattacks-experts-us-suleimani>

Historically, cyber-attacks between US and Iran have de-escalated conflict, but Suleimani killing may bring an end to that pattern.

The US assassination of Qassem Suleimani has increased the likelihood that a decade of cyber-hostilities between the US and Iran could escalate into true cyberwarfare, security experts have warned.

And with tensions mounting and Iran threatening "severe revenge" over the killing, concerns have arisen that blowback could come in the form of hacking attacks on critical infrastructure sectors, which include the power grid, healthcare facilities, banks and communications networks.

[Click link above to read more](#)

---

## Automotive cybersecurity incidents doubled in 2019, up 605% since 2016

<https://www.helpnetsecurity.com/2020/01/06/automotive-cybersecurity-incidents/>

Upstream Security's 2020 Automotive Cybersecurity Report shares in-depth insights and statistics gleaned from analyzing 367 publicly reported automotive cyber incidents spanning the past decade, highlighting vulnerabilities and insights identified during 2019.

"With the rapid rise of attacks on the automotive industry, OEMs and smart mobility providers need extensive visibility and clarity into the threat landscape, helping them design the proper security architecture spanning their vehicles and cloud environments," said Oded Yarkoni, Upstream Security's VP of Marketing. "Our annual automotive cybersecurity report shows that the threats faced by the entire industry are real and increasingly more prevalent."

[Click link above to read more](#)

---

## **Here are the top cybersecurity predictions for 2020**

<https://azbigmedia.com/business/technology/here-are-the-top-cybersecurity-predictions-for-2020/>

As 2019 comes to an end, cybersecurity experts are preparing for a new year—and a new decade—and all the cyber scams, breaches, attacks and privacy concerns that threaten consumers and businesses. CyberScout, an industry leader in cyber insurance, data security, and identity theft protection, continues to strengthen defenses against the constantly evolving cyber threats that will shape the 2020 security landscape, encouraging consumers and business owners to stay informed and aware.

[Click link above to read more](#)

---

## **Why is Brazil so vulnerable to cyber attacks?**

<https://www.bnamericas.com/en/features/why-is-brazil-so-vulnerable-to-cyber-attacks>

Year after year, Brazil continues to be a hotspot for a broad variety of cyberattacks, from phishing and DDoS campaigns to ransomware.

The number of cyberattacks on government networks increased again in 2019, according to data just released by government cyber incident handling and response center CTIR-Gov, a body linked to the office of institutional security (GSI).

[Click link above to read more](#)

---

## **Widely Known Flaw in Pulse Secure VPN Being Used in Ransomware Attacks**

<https://www.darkreading.com/attacks-breaches/widely-known-flaw-in-pulse-secure-vpn-being-used-in-ransomware-attacks/d/d-id/1336729>

New Year's Eve attack on currency exchange service Travelex may have involved use of the flaw.

VPN provider Pulse Secure on Monday urged customers to immediately apply a security patch if they have not yet done so. The company issued the patch last April to address a critical, remotely executable flaw in some versions of its products.

[Click link above to read more](#)

---

## **Malicious Google Play Apps Linked to SideWinder APT**

<https://www.darkreading.com/application-security/malicious-google-play-apps-linked-to-sidewinder-apt/d/d-id/1336728>

The active attack involving three malicious Android applications is the first exploiting CVE-2019-2215, Trend Micro researchers report.

Researchers have discovered an attack exploiting CVE-2019-2215, which leverages three malicious apps in the Google Play store to compromise a target device and collect users' data.

[Click link above to read more](#)

---

## **9 clever ways thieves steal your identity – and how you can stop them**

<https://www.foxnews.com/tech/9-clever-ways-thieves-steal-your-identity-and-how-you-can-stop-them>

Identity theft isn't just someone stealing your credit card. Criminals are coming up with plenty of innovative ways to rip us off. New account fraud, a tactic in which someone opens an account in your name, is on the rise. So are cases of hackers using clever social engineering tactics to fool victims into giving up sensitive information.

One recent example is a new type of identity fraud that tricks victims into thinking they've received a two-factor authentication text from their bank. This is especially shocking as it looks so real. Tap or click here to read all about it.

[Click link above to read more](#)

---

### Before you buy anything else on Amazon, read this important warning

<https://www.komando.com/lifestyle/before-you-buy-anything-else-on-amazon-read-this-important-warning/698371/>

Amazon is the marketplace to end all marketplaces. Not only has the company managed to disrupt most brick-and-mortar retail in the U.S., consumers actually prefer the tech-giant's approach to fast shipping and customer service.

In fact, Amazon is a winner for consumers in several categories. Each year, events like Prime Day rake in billions of dollars in sales. At the same time, the company is investing deeply in its infrastructure for technology like drone deliveries. Tap or click to see the future of Amazon's order fulfillment.

But not everything is rosy at Amazon right now. Customers are finding loads of dangerous counterfeit products for kids that can put young lives in danger. We'll show you what's going on. Plus, we'll talk about what "Amazon's choice" really means and why these products aren't always worth the hype.

[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.



 **Security News Digest**  
Information Security Branch

 **OCIO** | Office of the Chief Information Officer