January 21st, 2020

Try our January Quiz - Resolutions

Save the date - February 5th to 7th is the Privacy and Security Conference

This week's stories:

- Ottawa considering 'significant and meaningful' compensation for privacy breach victims
- What Are Third-Party Internet Cookies, and Why Is Google Killing Them?
- Windows 10 Has a Security Flaw So Severe the NSA Disclosed It
- 3 ways to browse the web anonymously
- U.S. firm Cloudflare offers free cybersecurity help to federal campaigns
- Ubisoft sues operators of four DDoS-for-hire services
- FBI shuts down website selling billions of stolen records
- How Cybercriminals Are Converting Cryptocurrency to Cash
- The case for cities that aren't dystopian surveillance states
- Artificial Fingerprint Ring Could Combat Biometric Data Theft

---

Ottawa considering 'significant and meaningful' compensation for privacy breach victims

https://www.cbc.ca/news/politics/privacy-breach-compensation-mandate-letter-1.5417467

Canadians who fall victim to privacy breaches could soon be eligible for some sort of compensation as the Liberal government works on introducing a new set of online rights.

Mandate letters for Innovation, Science and Industry Minister Navdeep Bains and Heritage Minister Steven Guilbeault say they've been asked by Prime Minister Justin Trudeau to work on a "digital charter" that would include legislation to give Canadians "appropriate compensation" when their personal data is breached.

It's not clear when the legislation will be introduced, or what a compensation package would even look like, but Bains said it will include punitive fines for those found guilty of breaching personal data.

Click link above to read more

What Are Third-Party Internet Cookies, and Why Is Google Killing Them?

https://www.vice.com/en_ca/article/5dmgkz/what-are-third-party-internet-cookies-and-why-is-google-killing-them

Google this week announced that the company will take steps to eventually eliminate third-party cookies, routinely used by data brokers to closely track and profit from your browsing behavior. But experts say that while the company's announcement is a good first step, the effort is belated, murky, and not quite the revolution it's being portrayed as.

In a blog post, Justin Schuh, Director of Chrome Engineering, announced that the company's Chrome browser would be moving away from using third-party cookies sometime in the next two years. First party

cookies would still be allowed, but third party cookies used to track you around the internet would eventually be banned.

Click link above to read more

Windows 10 Has a Security Flaw So Severe the NSA Disclosed It

https://www.wired.com/story/nsa-windows-10-vulnerability-disclosure/

Microsoft released a patch for Windows 10 and Server 2016 today after the National Security Agency found and disclosed a serious vulnerability. It's a rare but not unprecedented tip-off, one that underscores the flaw's severity—and maybe hints at new priorities for the NSA.

The bug is in Windows' mechanism for confirming the legitimacy of software or establishing secure web connections. If the verification check itself isn't trustworthy, attackers can exploit that fact to remotely distribute malware or intercept sensitive data

Click link above to read more

---

3 ways to browse the web anonymously

https://www.welivesecurity.com/2020/01/21/3-ways-browse-web-anonymously/

As concern about internet privacy grows and grows, more and more people are actively seeking to browse the web anonymously. There are various ways to avoid being identified or tracked on the internet, although, in fact, “attempt to avoid” might often be more appropriate. Online anonymity can often feel like a fleeting goal, and a problem as complex as online privacy has no solution that is bulletproof under all circumstances.

Besides rather simple options such as proxy services or virtual private networks (VPNs), there are other services that you can use in order to hide your surfing habits from your Internet Service Provider (ISP), government, or the very websites you’re visiting. Let’s look at the benefits and downsides of three easy-to-use anonymity networks – Tor, I2P, and Freenet.

Click link above to read more

U.S. firm Cloudflare offers free cybersecurity help to federal campaigns

https://www.ctvnews.ca/sci-tech/u-s-firm-cloudflare-offers-free-cybersecurity-help-to-federal-campaigns-1.4768114

A major U.S. web infrastructure and security company will provide free support to federal election campaigns to help thwart any repeats of the 2016 effort by Russian agents to steal and leak sensitive campaign emails and documents.

San Francisco-based Cloudflare said Wednesday it will be providing to eligible campaigns free access to several of its security services, including enhanced protection of firewalls, which defend systems and networks from unauthorized access. Other services include protection and mitigation of any denial-of-service attacks, which can paralyze a network by overwhelming it with data.

Click link above to read more

Ubisoft sues operators of four DDoS-for-hire services

https://www.zdnet.com/article/ubisoft-sues-operators-of-four-ddos-for-hire-services/

Gaming company Ubisoft has filed a lawsuit against five individuals for operating four DDoS-for-hire (DDoS booter) services that were used to launch DDoS attacks on Rainbow Six Siege multiplayer servers.
The legal complaint, filed last week, is the culmination of a months-long process that started back in September last year.

At the time, Ubisoft noticed a sharp increase in DDoS attacks targeting its Rainbow Six Siege (R6S) game. The reasons for the DDoS attacks was a new game update that just rolled out at the time, which also resulted in a reset of the global player ranking.

Click link above to read more

FBI shuts down website selling billions of stolen records

https://www.welivesecurity.com/2020/01/17/fbi-seizes-website-selling-stolen-personal-data/

US law enforcement has seized the WeLeakInfo.com domain name for peddling personal data stolen in data breaches. The shadowy website offered a pay-to-play scenario that allowed anyone to search for and access other people's personal details, according to a statement from the Department of Justice (DOJ).

WeLeakInfo.com "claimed to provide its users a search engine to review and obtain the personal information illegally obtained in over 10,000 data breaches containing over 12 billion indexed records," said the authorities

Click link above to read more

How Cybercriminals Are Converting Cryptocurrency to Cash

https://www.bankinfosecurity.com/how-cybercriminals-are-converting-cryptocurrency-to-cash-a-13625

Cybercriminals are using increasingly sophisticated methods to turn illicitly gained cryptocurrency into cash, which raises new concerns about enforcing anti-money laundering laws, according a report by blockchain analysis firm Chainalysis.

During 2019, analysts at Chainalysis traced $2.8 billion in bitcoin that criminal entities sent through cryptocurrency exchanges. They found that some exchanges known as "over-the-counter brokers" are being leveraged by cybercriminals to convert cryptocurrency that is paid out in ransomware and other attacks into cash for a fixed fee.

Click link above to read more

The case for cities that aren't dystopian surveillance states

https://www.theguardian.com/cities/2020/jan/17/the-case-for-cities-where-youre-the-sensor-not-the-thing-being-sensed

mart city" is one of those science fiction phrases seemingly designed to make you uneasy, like "neuromarketing" or "pre-crime". It's impossible to be alive in this decade and not find something unsettling in the idea of our cities becoming "smart".

It's not hard to see why: "smart" has become code for "terrible". A "smart speaker" is a speaker that eavesdrops on you and leaks all your conversations to distant subcontractors for giant tech companies. "Smart watches" spy on your movements and sell them to data-brokers for ad-targeting. "Smart TVs" watch you as you watch them and sell your viewing habits to brokers.

Click link above to read more

Artificial Fingerprint Ring Could Combat Biometric Data Theft

https://www.infosecurity-magazine.com/news/artificial-fingerprint-ring-created

A cybersecurity company has teamed up with a 3D accessory designer to produce a ring that could tackle the issue of what to do if your biometric data is stolen.

The attractive and wearable piece of jewelry features a synthetic fingerprint that can be used to unlock phones, make payments, or even access a home or office.

Unlike the actual fingerprint of a living human, which can never be replaced if lost, the artificial biometric identifier can be erased and substituted with a new version in the event of an identity theft.

The ring represents the collaborative efforts of cybersecurity firm Kaspersky, Swedish designer Benjamin Waye, and creative agency Archetype.

Click link above to read more

Click Unsubscribe to stop receiving the Digest.

****

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