




October 13^h, 2020

Challenge yourself during Cyber Security Awareness Month

Try our October - 'Cyber Security Awareness Month' Quiz

This week's stories:

- [Understanding Canadian cybersecurity laws: Peer-to-peer privacy protection — “Intrusion upon seclusion” and the protection of intimate images \(Article 6\)](#) 
- [Treasury Dept. Advisory Shines Spotlight on Ransomware Negotiators](#)
- [The use of biometrics is accelerating and outpacing legislation](#)
- [Contract changes needed to improve cybersecurity, Space Force leader says](#)
- [DHS warns that Emotet malware is one of the most prevalent threats today](#)
- [The Digital Transformation Reckoning Caused By COVID-19](#)
- [Microsoft October 2020 Patch Tuesday fixes 87 security bugs](#)
- [NCSAM: Hybrid Workforce and its Cybersecurity Implications](#)
- [5 steps to secure your connected devices](#)

Understanding Canadian cybersecurity laws: Peer-to-peer privacy protection — “Intrusion upon seclusion” and the protection of intimate images (Article 6) 

<https://www.itworldcanada.com/blog/understanding-canadian-cybersecurity-laws-peer-to-peer-privacy-protection-intrusion-upon-seclusion-and-the-protection-of-intimate-images-article-6/437022>

The prevalence of digital communication has created nearly limitless possibilities for the rapid, large-scale sharing of private communications, intimate images, and personal information. Through the use of online tools and social media applications, access to the internet can be used to turn a small threat within an interpersonal dispute into a viral media publication; downloaded, viewed, and retransmitted to millions of people around the world. In the modern age of high-speed information sharing, privacy and the ability to control the information which is publicly shared about yourself has become increasingly imperative. Not only can the intrusion upon your personal information feel harmful and disruptive to your personal and professional reputation, but the use of visual recordings of intimate images has also been weaponized as a tool for criminal acts of extortion and cyberbullying, and has quickly become a contributing factor to an increase of suicides and suicide attempts amongst our young Canadians.

[Click link above to read more](#)

Treasury Dept. Advisory Shines Spotlight on Ransomware Negotiators

<https://threatpost.com/zerologon-attacks-microsoft-dcs-snowball/159656/https://www.darkreading.com/attacks-breaches/treasury-dept-advisory-shines-spotlight-on-ransomware-negotiators/d/d-id/1339169>

The emerging ransomware negotiator industry has come into the spotlight recently following an advisory from the US Department of the Treasury for companies that facilitate ransom payments to threat actors on behalf of victims.

The advisory, from the department's Office of Foreign Assets Control (OFAC), warned of potential regulatory trouble that such organizations could face if ransom payments ended up in the hands of adversaries on OFAC's Specially Designated Nationals and Blocked Persons List (SDN). US persons and entities are prohibited from conducting transactions with anyone on the SDN list or with any individual or organizations from countries that OFAC has officially sanctioned, such as North Korea, Iran, Ukraine, and Syria.

[Click link above to read more](#)

The use of biometrics is accelerating and outpacing legislation

<https://cybernews.com/privacy/the-use-of-biometrics-is-accelerating-and-outpacing-legislation/>

Last year, FaceApp made headlines. The Russian-made app was allegedly transferring people's personal photos to Russia and, allegedly, used them for geopolitical purposes. Ultimately, reminded Melissa Wingard, it became clear the allegations were unfounded, and the app wasn't using the data for foreign affairs purposes.

But the scandal got Mellisa Wingard thinking about how often we are sharing our biometric data, and who we are sharing it with. Also, what are we getting in return?

"Privacy is a fundamental human right, and we should be cherishing it," said Melissa Wingard during the Black Hat Asia 2020 summit.

[Click link above to read more](#)

Contract changes needed to improve cybersecurity, Space Force leader says

<https://washingtontechnology.com/articles/2020/10/07/space-force-cyber-thompson.aspx>

The U.S. Space Force is working on bolstering its space and missile systems' cybersecurity, starting with its infrastructure contracts.

Lt. Gen. John Thompson, commander of the Space and Missile Systems Center (SMSC) under the U.S. Space Force, said cybersecurity was increasingly integral to space missions as threats continue to grow during the California Polytechnic State University's Space and Cybersecurity Symposium Oct. 5.

[Click link above to read more](#)

DHS warns that Emotet malware is one of the most prevalent threats today

<https://arstechnica.com/information-technology/2020/10/dhs-warns-that-emotet-malware-is-one-of-the-most-prevalent-threats-today/>

The malware known as Emotet has emerged as “one of the most prevalent ongoing threats” as it increasingly targets state and local governments and infects them with other malware, the cybersecurity arm of the Department of Homeland Security said on Tuesday.

Emotet was first identified in 2014 as a relatively simple trojan for stealing banking account credentials. Within a year or two, it had reinvented itself as a formidable downloader or dropper that, after infecting a PC, installed other malware. The Trickbot banking trojan and the Ryuk ransomware are two of the more common follow-ons. Over the past month, Emotet has successfully burrowed into Quebec’s Department of Justice and increased its onslaught on governments in France, Japan, and New Zealand. It has also targeted the Democratic National Committee.

[Click link above to read more](#)

The Digital Transformation Reckoning Caused By COVID-19

<https://www.infosecurity-magazine.com/opinions/digital-transformation-covid19/>

For many companies, the goal for the first half of this year was simple: digitally transform, or risk going out of business. This meant, to continue functioning amid a raging pandemic, they needed to execute “emergency digital transformations” to enable employees to work from home, and to enable formerly manual processes to be conducted digitally.

In fact, a May 2020 survey conducted by [MariaDB](#) found that 40% of respondents are fast-tracking their move to the cloud due to COVID-19.

[Click link above to read more](#)

Microsoft October 2020 Patch Tuesday fixes 87 security bugs

<https://www.bleepingcomputer.com/news/security/microsoft-october-2020-patch-tuesday-fixes-87-security-bugs/>

Today is Microsoft’s October 2020 Patch Tuesday, and your Windows administrators will be pulling their hair out as they install new updates and try to fix bugs that pop up.

With the October 2020 Patch Tuesday security updates release, Microsoft has released fixes for 87 vulnerabilities in Microsoft products and an advisory about [today's Adobe Flash Player update](#).

[Click link above to read more](#)

NCSAM: Hybrid Workforce and its Cybersecurity Implications

<https://cisomag.eccouncil.org/hybrid-workforce-cybersecurity-implications/>

In an interview at the TIME100 Honorees: Visions for the Future event, Alphabet CEO Sundar Pichai [said](#) “We firmly believe that in-person, being together, having a sense of community is super important when you have to solve hard problems and create something new so we don’t see that changing. But we do think we need to create more flexibility and more hybrid models.” It is safe to say that the pandemic has changed the workforce for good, and a hybrid model— a blend of both remote and in-office methods of working, will eventually take precedence. But the security of a hybrid model is still a far cry. During this year’s National Cybersecurity Awareness Month, let us look at how the changing workforce dynamics will change cybersecurity for good.

[Click link above to read more](#)

5 steps to secure your connected devices

<https://www.welivesecurity.com/2020/10/05/5-steps-secure-connected-devices/>

As we aim to make our lives simpler to manage, especially in this hurried day and age, we increasingly rely on our connected devices. With Internet of Things (IoT) and smart devices becoming cheaper and more accessible to the masses, it's easier to incorporate them into our lives. Let's be honest, who hasn't used their smartphone-based voice assistant to dictate a note or jot down an appointment in their calendar? Or for that matter, made additions to their household in the form of smart devices; smart televisions, for one, are hard to avoid nowadays.

However, the proliferation of all these devices in our everyday lives also poses a security risk, as the gadgets and gizmos, unless secured properly, can be used as new avenues of attack by cybercriminals. So, what steps can you take to ensure the security of your internet-connected devices and mitigate the chances of falling victim to a cyberattack? As [Cyber Security Awareness Month \(CSAM\) is upon us](#), we highlight the ways you can protect yourself. After all, the initiative's key message this year is: "If you connect it, protect it."

[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.

