




September 15th, 2020
Try our September - 'Passwords' Quiz

This week's stories:

- [U of T's partnership with Alibaba raises privacy concerns](#) 
- [CEOs Could Face Jail Time for IoT Attacks by 2024](#)
- [CISA: Chinese Hackers Exploiting Unpatched Devices to Target U.S. Agencies](#)
- [Misconfigured Database Leaks 370 Million Dating Site Records](#)
- [New Twitter phishing scam inspired from Twitter's latest security response](#)
- [Surge in DDoS attacks targeting education and academic sector](#)
- [Staples discloses data breach exposing customer info](#)
- [New Windows exploit lets you instantly become admin. Have you patched?](#)

U of T's partnership with Alibaba raises privacy concerns

<https://thevarsity.ca/2020/09/07/opinion-u-of-ts-partnership-with-alibaba-raises-privacy-concerns/>

COVID-19 has changed the way we learn, as many U of T students are studying completely online for this academic year. Beyond the numerous administrative headaches and technological glitches this introduces, this move also opens the door to another complication: data privacy.

On July 9, the University of Toronto initiated a partnership with Chinese conglomerate Alibaba to use its Cloud Enterprise Network (CEN). This service was designed to provide students studying from mainland China with faster, more reliable, and more consistent access to U of T services like Quercus and Blackboard Collaborate.

[Click link above to read more](#)

CEOs Could Face Jail Time for IoT Attacks by 2024

<https://www.infosecurity-magazine.com/news/ceos-face-jail-time-iot-attacks-by>

Corporate CEOs could soon be personally liable if they fail to adequately secure IT systems connected to the physical world, Gartner has warned.

The analyst firm predicted that as many as 75% of business leaders could be held liable by 2024 due to increased regulations around so-called "cyber-physical systems" (CPSs) such as IoT and operational technology (OT).

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

CISA: Chinese Hackers Exploiting Unpatched Devices to Target U.S. Agencies

<https://thehackernews.com/2020/09/chinese-hackers-agencies.html>

The US Cybersecurity and Infrastructure Security Agency (CISA) issued a new advisory on Monday about a wave of cyberattacks carried by Chinese nation-state actors targeting US government agencies and private entities.

"CISA has observed Chinese [Ministry of State Security]-affiliated cyber threat actors operating from the People's Republic of China using commercially available information sources and open-source exploitation tools to target US Government agency networks," the cybersecurity agency said.

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

Misconfigured Database Leaks 370 Million Dating Site Records

<https://www.infosecurity-magazine.com/news/misconfigured-database-leaks-370/>

Global users of 70+ dating and e-commerce sites have had their personal data exposed after a popular marketing software provider misconfigured an online database.

Discovered by an ethical hacker and reported to vpnMentor, the issue is an unsecured and unencrypted Elasticsearch database, managed by Cyprus-headquartered Mailfire.

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

New Twitter phishing scam inspired from Twitter's latest security response

<https://www.hackread.com/twitter-phishing-scam-latest-security-response/>

Crooks are using the July 15th's cyberattack on Twitter to carry out phishing scam designed to steal the login credentials of unsuspected users.

Twitter for the past year or so has been constantly embroiled in a range of controversies. Earlier this month Indian Prime Minister Modi's personal yet verified Twitter account was hacked while in July, we saw how 130 accounts of high profile individuals were hacked resulting in attackers siphoning large amounts of cryptocurrencies from innocent users.

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

Surge in DDoS attacks targeting education and academic sector

<https://www.bleepingcomputer.com/news/security/surge-in-ddos-attacks-targeting-education-and-academic-sector/>

As education institutions across the world moved to online learning, cyber threat disruptions have amplified more than ever. Malware, vulnerability exploits, distributed denial-of-service (DDoS), phishing attacks have all struck this sector, increasing in frequency over the past two months.

As schools in the U.S. restarted in remote learning mode, cybersecurity companies noticed a surge in DDoS attacks causing network downtime and pausing classes as a consequence.

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

Staples discloses data breach exposing customer info

<https://www.bleepingcomputer.com/news/security/staples-discloses-data-breach-exposing-customer-info/>

Giant office retail company Staples informed some of its customers that data related to their orders has been accessed without authorization.

Few details are available at the moment. The company has not disclosed the incident publicly and alerted affected customers individually over email.

[Click link above to read more](#)

New Windows exploit lets you instantly become admin. Have you patched?

<https://arstechnica.com/information-technology/2020/09/new-windows-exploit-lets-you-instantly-become-admin-have-you-patched/>

Researchers have developed and published a proof-of-concept exploit for a recently patched Windows vulnerability that can allow access to an organization's crown jewels—the Active Directory domain controllers that act as an all-powerful gatekeeper for all machines connected to a network.

CVE-2020-1472, as the vulnerability is tracked, carries a critical severity rating from Microsoft as well as a maximum of 10 under the Common Vulnerability Scoring System. Exploits require that an attacker already have a foothold inside a targeted network, either as an unprivileged insider or through the compromise of a connected device.

[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.

