

August 2, 2022

Challenge yourself with our [Summer Social Media Security quiz!](#)

[This past week's stories:](#)

 [3 Toronto arts companies among those impacted by email newsletter cyber attack](#)

[Infostealer malware targets Facebook business accounts to capture sensitive data](#)

[Cybersecurity vendor Entrust tells customers data was stolen during June cyberattack](#)

[1 in 3 employees don't understand why cybersecurity is important](#)

[NFT hacking group attacks on the rise, report finds](#)

[US govt warns Americans of escalating SMS phishing attacks](#)

[U.S. Justice Department probing cyber breach of federal court records system](#)

[Cybrary secures \\$25M to grow its platform for cybersecurity training](#)

[Tips for translating cyber risk into board-friendly language](#)

[Identifying cybersecurity issues in your business](#)

[Yale to partner in NSF program advancing cybersecurity and privacy](#)

[The four cybersecurity lessons to teach schools](#)

[Taiwanese websites hit with DDoS attacks as Pelosi begins visit](#)

3 Toronto arts companies among those impacted by email newsletter cyber attack

Several Toronto-based arts companies have been hit as part of a data breach impacting an email newsletter distribution service.

The Canadian Opera Company, Toronto Symphony Orchestra and Canadian Stage all emailed subscribers to inform them of a ransomware attack suffered by WordFly.

<https://globalnews.ca/news/9020078/toronto-arts-organizations-ransom-ware-data/>

Click above link to read more.

[Back to top](#)

Infostealer malware targets Facebook business accounts to capture sensitive data

Social media is one area that cybercriminals love to exploit to attack their victims. And as one of the most popular social networks, Facebook is often in the crosshairs of malware campaigns. A new attack analyzed by cybersecurity provider WithSecure Intelligence targets Facebook business users with the intent of stealing their sensitive data and taking over their accounts.

Using Facebook's Meta Business Suite, organizations can designate specific employees to communicate with customers, discuss their products and services and create ads to run on Facebook. In the malicious campaign dubbed Ducktail, cybercriminals look for companies that use Facebook's Business/Ads platform and then target people within the company who may have high-level access to the business accounts. Among the employees singled out in this campaign have been ones in management, digital marketing, digital media and human resources, according to WithSecure.

https://www.techrepublic.com/article/infostealer-malware-targets-facebook-business-accounts-to-capture-sensitive-data/?utm_source=email&utm_medium=referral&utm_campaign=cybersecurity-insider

Click above link to read more.

[Back to top](#)

Cybersecurity vendor Entrust tells customers data was stolen during June cyberattack

Minneapolis-based cybersecurity giant Entrust has confirmed it was hit by a cyberattack last month.

Entrust, which describes itself as a global leader in identities, payments and data protection, told TechCrunch that an "unauthorized party" was able to access parts of its system that are used for the internal operations on June 18.

<https://techcrunch.com/2022/07/27/entrust-data-stolen-june-cyberattack/>

Click above link to read more.

[Back to top](#)

1 in 3 employees don't understand why cybersecurity is important

According to a new Tessian report, 30% employees do not think they personally play a role in maintaining their company's cybersecurity posture.

What's more, only 39% of employees say they're very likely to report a security incident, making investigation and remediation even more challenging and time-consuming for security teams. When asked why, 42% of employees said they wouldn't know if they had caused an incident in the first place, and 25% say they just don't care enough about cybersecurity to mention it.

<https://www.helpnetsecurity.com/2022/07/28/employees-dont-understand-why-cybersecurity-is-important/>

Click above link to read more.

[Back to top](#)

NFT hacking group attacks on the rise, report finds

Web3 Security firm TRM Labs has said that attacks carried out on NFT projects implemented through their Discord channels have risen significantly. Most of these attacks are, reportedly, associated with a "wider group" of hackers.

In the last two months, over 100 reports of Discord channel hacks have been filed with Chainabuse, a community-led scam reporting platform operated by TRM Labs. Worryingly, in May alone the losses were reported to have been worth more than \$22 million.

<https://www.itsecurityguru.org/2022/07/27/nft-hacking-group-attacks-on-the-rise-report-finds/>

Click above link to read more.

[Back to top](#)

US govt warns Americans of escalating SMS phishing attacks

The Federal Communications Commission (FCC) warned Americans of an increasing wave of SMS (Short Message Service) phishing attacks attempting to steal their personal information and money.

Such attacks are also known as smishing or robotexts (as the FCC calls them), and scammers behind them may use various lures to trick you into handing over confidential information.

<https://www.bleepingcomputer.com/news/security/us-govt-warns-americans-of-escalating-sms-phishing-attacks/>

Click above link to read more.

[Back to top](#)

U.S. Justice Department probing cyber breach of federal court records system

The U.S. Justice Department is investigating a cyber breach involving the federal court records management system, the department's top national security attorney told lawmakers on Thursday.

Matt Olsen, head of the Justice Department's National Security Division, alluded to the threat of cyber attacks by foreign nations as he told the U.S. House of Representative Judiciary Committee that the incident was a "significant concern."

<https://www.reuters.com/world/us/us-justice-dept-probing-cyber-breach-federal-court-management-system-2022-07-28/>

Click above link to read more.

[Back to top](#)

Cybrary secures \$25M to grow its platform for cybersecurity training

The cybersecurity industry has taken a hit recently, with economic headwinds prompting layoffs and a broad investor pullback. But some firms have escaped unscathed, like cybersecurity training platform Cybrary, which today announced that it raised \$25 million in a Series C funding round. CEO Kevin Hanes conveyed to TechCrunch that the round, which brings Cybrary's total raised to \$48 million, was led by BuildGroup and Gula Tech Adventure and will be put toward developing "content and capabilities" on the company's platform.

Cybrary was launched in 2015 by co-founders Ralph Sita and Ryan Corey (Hanes joined as CEO a year ago). As Hanes tells it, their mission was to break down barriers to the cybersecurity industry by creating a way for aspiring professionals to enter the field — no matter their background or experience.

<https://techcrunch.com/2022/08/02/cybrary-secures-25m-to-grow-its-platform-for-cybersecurity-training/>

Click above link to read more.

[Back to top](#)

Tips for translating cyber risk into board-friendly language

CISOs finally have a seat at the table. Recent high-profile cyberattacks have forced C-suites to pay close attention to cybersecurity, elevating the role of the CISO. But this new rise to prominence doesn't mean CISOs are exactly seeing eye-to-eye with their boards.

One reason behind this growing disconnect is the difference in perspectives: CISOs and board members often do not speak the same business language.

<https://www.cybersecuritydive.com/news/board-cyber-risk-ciso/628543/>

Click above link to read more.

[Back to top](#)

Identifying cybersecurity issues in your business

Threats to your business come in many forms. For most organizations, the biggest threats to their survival are related to cybersecurity. An Allianz survey found this to be true, as "cyber incidents" ranked as the biggest risk to organizations, overtaking "business interruption". Whether those threats are external or internal, they are continuous and evolving because of the ever-increasing shift towards digital.

Over 98 percent of UK security professionals have reported an increase in cyber-attacks against their businesses in the past year. A further 96 percent say those attacks have become more sophisticated. This shows the need for constantly-evolving UK cybersecurity.

<https://betanews.com/2022/08/01/cybersecurity-issues-in-business/>

Click above link to read more.

[Back to top](#)

Yale to partner in NSF program advancing cybersecurity and privacy

Yale University is among the key partners of the Secure and Trustworthy Cyberspace program, a \$25.4 million multi-institutional effort supported by the National Science Foundation (NSF) that seeks to advance ambitious research and center-scale projects in cybersecurity and privacy.

"The Secure and Trustworthy Cyberspace program is one of NSF's largest research programs, recognizing the criticality of cybersecurity and privacy to the nation's economy and to citizens," said NSF Director Sethuraman Panchanathan. "These investments support cybersecurity research across the country that can be translated into solutions that improve our quality of life."

<https://seas.yale.edu/news-events/news/yale-partner-nsf-program-advancing-cybersecurity-and-privacy>

Click above link to read more.

[Back to top](#)

The four cybersecurity lessons to teach schools

With schools out for summer, the education sector can't quite switch off yet. Several high-profile cyber attacks have put education systems on edge. The Kellogg Community College cyberattack in Michigan, which severely disrupted IT services, cancelling classes and exams in the process, shows there is still much to be done to protect the education sector.

The sector has been a prominent cyber target for a while, the higher education sector in particular, due to research programs that house valuable data. A 2022 Mid-Year Threat Report finds that ransomware attacks have climbed 51% since last year, while malware is up 22%. A recent survey found that a third of UK schools lack cybersecurity policies. Another example dates only back to May 2022, when a breach of education software provider Illuminate Education exposed data of over 1 million current and former students across New York State. According to recent data from SonicWall in 2021, the education industry saw a 152% increase in ransomware attacks; and an average of 22% were targeted by malware attacks each month. Clearly, cyberattacks are relentlessly rising.

<https://www.fenews.co.uk/fe-voices/the-four-cybersecurity-lessons-to-teach-schools/>

Click above link to read more.

[Back to top](#)

Taiwanese websites hit with DDoS attacks as Pelosi begins visit

Key Taiwanese websites experienced intermittent outages Tuesday due to some minor cyberattacks just ahead of House Speaker Nancy Pelosi's arrival in Taiwan.

The attacks hit at least four websites — those of President Tsai Ing-wen, the National Defense Ministry, the Foreign Affairs Ministry and the country's largest airport, Taiwan Taoyuan International.

<https://www.nbcnews.com/tech/security/taiwanese-websites-hit-ddos-attacks-pelosi-begins-visit-rcna41144>

Click above link to read more.

[Back to top](#)

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.

