## July 26, 2022

**Challenge yourself with our [Travel Security](#) quiz!**

This past week's stories:

🍁 **['Cyber security incident' in St. Marys](#)**

🍁 **[Governments must do more to fight ransomware, says insurance industry](#)**

🍁 **[Majority of Canadian parents trust their kids to go online unmonitored: Survey](#)**

**[China fines Didi $1.2 billion for violating cybersecurity and data laws](#)**

**[Cyber security school launched in PH](#)**

**[Australia more concerned about cybersecurity than rest of the world: PwC](#)**

**[Free entry-level cybersecurity course to be made available to 1m people](#)**

**[Ukrainian radio stations hacked to broadcast fake news about Zelenskyy's health](#)**

**[North Aurora woman scammed out of $230K accused of crimes she didn't commit](#)**

**[Uber admits covering up 2016 hacking, avoids prosecution in U.S. settlement](#)**

**[LinkedIn remains the most impersonated brand in phishing attacks](#)**

**[Italy investigating ransomware attack on tax agency](#)**

**[The growth in targeted, sophisticated cyberattacks troubles top FBI cyber official](#)**

---

### 'Cyber security incident' in St. Marys

The Town of St. Marys is investigating what is being described as a "cyber security incident" that has locked the town's internal server and encrypted its data.

According to a release, the incident happened on July 20 and staff took immediate steps to secure any sensitive information, including locking down the Town's IT systems and restricting access to email. The Town also notified its legal counsel, the Stratford Police Service and the Canadian Centre for Cyber Security.

https://london.ctvnews.ca/cyber-security-incident-in-st-marys-1.5998416

*Click above link to read more.*

Back to top

---

**Governments must do more to fight ransomware, says insurance industry**

Governments and regulators have to do more to counter groups and individuals behind ransomware attacks, says a group representing global insurance companies.

The recommendation is one of several made in a report on ransomware and cyber insurance issued Tuesday by the Geneva Association. It also says forbidding organizations from paying ransoms for the return of access to stolen data "is a blunt, potentially ineffective instrument."

https://www.itworldcanada.com/article/governments-must-do-more-to-fight-ransomware-says-insurance-industry/493584

*Click above link to read more.*

Back to top

---

**Majority of Canadian parents trust their kids to go online unmonitored: Survey**

As more children under the age of 18 use the internet, a majority of Canadian parents trust them to go online without supervision, but have concerns about their safety, according to a new global survey.

According to the 2022 Norton Cyber Safety Insights Report released Tuesday, 69 per cent of surveyed Canadian parents say they "trust their children to browse the internet unmonitored," and 86 per cent say it is "absolutely essential" to teach children about cyber safety.

https://www.ctvnews.ca/lifestyle/majority-of-canadian-parents-trust-their-kids-to-go-online-unmonitored-survey-1.5995850

*Click above link to read more.*

Back to top

---

## China fines Didi $1.2 billion for violating cybersecurity and data laws

China's cyberspace regulator fined Didi Global just over 8 billion yuan ($1.2 billion) on Thursday for violating cybersecurity and data laws, putting an end to a yearlong investigation into the ride-hailing giant.

The Cyberspace Administration of China (CAC) said in a statement that the firm had breached the country's cybersecurity law, data security law, and personal information protection law.

https://www.cnn.com/2022/07/21/economy/china-fines-didi-data-law-violation-intl-hnk/index.html

*Click above link to read more.*

Back to top

## Cyber security school launched in PH

The first globally-accredited cyber school was launched in Manila Wednesday, bringing in Israeli cyber security education to the Philippines.

The CybersCool Defcon will offer programs based on modules developed by Tel Aviv-based ThriveDX Saas, a company founded by Roy Zur, who previously spearheaded the design and training of elite Israeli Cyber and Intelligence Units.

https://www.pna.gov.ph/articles/1179443

*Click above link to read more.*

Back to top

## Australia more concerned about cybersecurity than rest of the world: PwC

Australian business leaders are more concerned about cybersecurity risks than their global counterparts, despite local interest rate hikes, inflation, supply chain disruptions, extreme weather events and the ongoing Covid-19 pandemic, according to new PwC research.

PwC's Global Risk Survey reveals that cyber and information management is considered the top risk to Australian business (32 percent compared to 20 percent globally), followed by business operating model, geopolitical risks, recruiting and retaining talent and managing the current workforce.

https://www.itnews.com.au/digitalnation/news/australia-more-concerned-about-cybersecurity-than-rest-of-the-world-pwc-582980

*Click above link to read more.*

---

**Free entry-level cybersecurity course to be made available to 1m people**

Cybersecurity non-profit (ICS)2 has been piloting a cybersecurity professional certificate for beginners and is now rolling it out further.

(ISC)2, an international non-profit organisation for cybersecurity professionals, is expanding its free entry-level cybersecurity professional education programme to 1m people.
The organisation's plan is to make the programme available on a larger scale globally to combat the worldwide skills shortage in the industry. Last year, it estimated that Ireland needs 10,000 more cybersecurity workers to plug skills gaps.

https://www.siliconrepublic.com/careers/ics2-cybersecurity-free-course

*Click above link to read more.*

---

**Ukrainian radio stations hacked to broadcast fake news about Zelenskyy's health**

Ukrainian radio operator TAVR Media on Thursday became the latest victim of a cyberattack, resulting in the broadcast of a fake message that President Volodymyr Zelenskyy was seriously ill.

"Cybercriminals spread information that the President of Ukraine, Volodymyr Zelenskyy, is allegedly in intensive care, and his duties are performed by the Chairman of the Verkhovna Rada, Ruslan Stefanchuk," the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) said in an update.

https://thehackernews.com/2022/07/ukrainian-radio-stations-hacked-to.html

*Click above link to read more.*

---

**North Aurora woman scammed out of $230K accused of crimes she didn't commit**

A North Aurora senior citizen is accused of money laundering and drug trafficking but it's not true.

To clear her name, she needed to deposit hundreds of thousands of dollars into a new account opened for her.

https://www.cbsnews.com/chicago/news/north-aurora-woman-scammed-230k/

*Click above link to read more.*

Back to top

---

## Uber admits covering up 2016 hacking, avoids prosecution in U.S. settlement

Uber Technologies Inc (UBER.N) on Friday accepted responsibility for covering up a 2016 data breach that affected 57 million passengers and drivers, as part of a settlement with U.S. prosecutors to avoid criminal charges.

In entering a non-prosecution agreement, Uber admitted that its personnel failed to report the November 2016 hacking to the U.S. Federal Trade Commission, even though the agency had been investigating the ride-sharing company's data security.

https://www.reuters.com/business/autos-transportation/uber-enters-non-prosecution-agreement-admits-covering-up-2016-data-breach-2022-07-22/

*Click above link to read more.*

Back to top

---

## LinkedIn remains the most impersonated brand in phishing attacks

LinkedIn is holding the top spot for the most impersonated brand in phishing campaigns observed during the second quarter of 2022.

Statistical data from cybersecurity company Check Point shows that the social platform for professionals is at the top of the list for the second quarter in a row.

https://www.bleepingcomputer.com/news/security/linkedin-remains-the-most-impersonated-brand-in-phishing-attacks/

*Click above link to read more.*

Back to top

**Italy investigating ransomware attack on tax agency**

Prolific ransomware group LockBit added Italy's tax agency to its list of victims this weekend, but the company investigating the alleged attack said Monday there was no evidence of a breach.

L'Agenzia delle Entrate did not respond to requests for comment but released a statement on Monday saying it asked Sogei, an IT company owned by the Ministry of Economy and Finance, to investigate the alleged ransomware attack.

https://therecord.media/italy-investigating-ransomware-attack-on-tax-agency/

*Click above link to read more.*

Back to top

**The growth in targeted, sophisticated cyberattacks troubles top FBI cyber official**

The FBI is deeply worried that cybercriminals and nation-state adversaries are developing more precision in their attacks and taking advantage of innovations in artificial intelligence that will compound the digital threat in the years to come, FBI Assistant Director for Cyber Bryan Vorndran said Wednesday.

"When we think about software as a service or even supply chain attacks, what happens when the adversary understands that there is perhaps one software factory that services the entire community," said Vorndran, who oversees 1,000 FBI agents focused on cybercrimes nationwide, during a speech Wednesday at a Fordham University cybersecurity conference.

https://www.cyberscoop.com/fbi-worries-about-future-cyber-threats/

*Click above link to read more.*

Back to top