BRITISH COLUMBIA OCIO Office of the Chief Information Officer

Security News Digest

May 1st, 2018

May is Password Protection Month

Take our quiz and test your knowledge

On this day in history (May 1st)

1975 – As the Vietnam War ends, Canada agrees to admit 3,000 South Vietnamese refugees.

2007 – The House of Commons unanimously apologizes to former students of Canada's Residential Schools.

This week's stories:

RCMP involved in closing of world's biggest DDoS-for-hire site

Rogers, Bell and Public Safety refused interviews on phone hack - but talked about it in private

Researchers Find Amazon Alexa Can Be Hacked to Record Users

YouTube ran ads from over 300 companies on extremist, white nationalist channels

Majority of large charities have experienced cyber attacks

ISO blocks NSA's latest IoT encryption systems amid murky tales of backdoors and bullying

More than 1 million kids had their identities stolen in 2017

China using water spray, facial recognition technology to stop jaywalkers

RCMP involved in closing of world's biggest DDoS-for-hire site

https://www.itworldcanada.com/article/rcmp-involved-in-closing-of-worlds-biggest-ddos-for-hire-site/404579

The RCMP was involved in action by several police forces this week who shut down what they say was the world's biggest Distributed Denial of Service (DDoS) website.

The Mounties said they executed a search warrant in Toronto as part of the takedown Tuesday of Webstresser.org, linked to more than four million cyber attacks across the globe. One was a massive attack against seven of the U.K.'s biggest banks in November, 2017. The banks were forced to reduce operations or shut down entire systems, police said, and had to pay hundreds of thousands of dollars to get services back up and running.

Europol said the six administrators of the site were located in the United Kingdom, Croatia, Canada and Serbia and that charges were laid. However, the RCMP press release made no mention of criminal charges laid here.

Europol also said unspecified "further measures" were taken against the top users of this marketplace in the Netherlands, Italy, Spain, Croatia, the United Kingdom, Australia, Canada and Hong Kong.

After the arrests Dutch police, with assistance from Germany and the United States, then seized servers and effected a takedown of the website Tuesday morning.

[Read the rest of the article online to learn more]

Rogers, Bell and Public Safety refused interviews on phone hack - but talked about it in private

http://www.cbc.ca/news/politics/bell-rogers-dube-hack-lobbying-1.4628806

After a CBC News/Radio-Canada investigation in November showed how relatively easy it was to hack phones on the Bell and Rogers mobile networks, **the telecom companies and Public Safety Canada refused to grant interviews.**

Instead, they chose to talk about the issue among themselves and in private, according to the federal lobbying registry.

The November investigation showed that, using only the number of his mobile phone, it was possible to intercept the calls and movements of Quebec NDP MP Matthew Dubé.

The NDP's public safety and emergency preparedness critic had agreed to let his telephone be hacked as part of the investigation.

The phone was connected to the Rogers mobile network, but CBC News/Radio-Canada journalists were also able to successfully hack Bell Canada's network.

The hack was done with the help of cybersecurity experts in Germany who exploited a weakness in the global telecommunications networks' Signalling System No. 7, or SS7. Any network that fails to adopt adequate security measures is vulnerable to hacking through SS7.

In November, CBC/Radio-Canada requested interviews with both Bell and Rogers to discuss a vulnerability in the SS7 system that puts the privacy of their subscribers at risk. The two companies refused to speak publicly and limited their responses to brief emails.

Public Safety Minister Ralph Goodale also refused an interview, claiming that SS7's flaws are not among his ministry's responsibilities.

[Read the rest of the article online to learn more]

Researchers Find Amazon Alexa Can Be Hacked to Record Users

http://www.eweek.com/security/researchers-find-amazon-alexa-can-be-hacked-to-record-users

On April 25, security firm Checkmarx publicly disclosed that it has found that a malicious developer can trick Amazon's Alexa voice assistant technology to record everything a user says.

At this time, it's not clear if any hackers have ever exploited the flaw, which is not in the Amazon Echo hardware, but rather is an abuse of functionality in the Alexa Skills feature set. Developers can extend Alexa's technology by building skills that provide new functionality for end users. Checkmarx found that there were several unbounded parameters that were **available to Alexa skills developers that could have enabled a malicious developer to record and even transcribe what a user says, even after the user had finished communicating with the device.**

"Customer trust is important to us, and we take security and privacy seriously," an Amazon spokesperson wrote in an email to eWEEK. "We have put mitigations in place for detecting this type of skill behavior and reject or suppress those skills when we do."

This isn't the first time a security researcher has raised the alarm about the potential for using Alexa-powered devices to eavesdrop. In August 2017, security researcher Mark Barnes with MWR Labs released a reporton a similar risk, although an attacker would need physical access to the device. In the Checkmarx research, **an attacker could manipulate an Alexa Skill, which can be installed by unsuspecting users and doesn't require any physical access or tampering with the Amazon Echo smart speaker.**

"The problem is that the attack we described leaves no trace, so a naïve user will not be able to know," Erez Yalon, manager of application security research at Checkmarx, told eWEEK. "It makes sense that with the info they have now, Amazon can check if the Amazon Store hosts any malicious Alexa Skills."

[Read the rest of the article online to learn more]

YouTube ran ads from over 300 companies on extremist, white nationalist channels: Report

https://globalnews.ca/news/4160033/youtube-ads-extremist-white-nationalist/

Earlier this year, YouTube pledged to demonetize videos that contained “inappropriate content,” but **a recent CNN investigation has revealed that advertisements from over 300 major companies have continued to appear before videos depicting extremist, white nationalist or other hateful content.**

Content featured on those channels include videos promoting white nationalists, Nazis, pedophilia, conspiracy theories, North Korean propaganda, among other things, CNN reports.

According to reports, many of the companies were not aware that their ads were being run on videos of this nature and said they’d be investigating how they wound up there. Incidents have cropped up over the past year that have sparked questions about YouTube’s ability to monitor ad placement on its platform.

Companies that advertise on YouTube have the option to target ads according to user base and demographic. CNN also reports that companies can stop their ads from appearing on videos posted by specific channels, and can select a “sensitive subject exclusion filter.”

For the past year, YouTube has repeatedly come under fire for extremist content on its platform, and more recently, for allowing those channels to monetize their videos. **In response, several companies have scaled back their use of YouTube advertising, while others have pledged to abandon the platform.**

Sportswear company Under Armour, for example, told CNN that it would be working with YouTube to prevent this from happening after the company was notified that its ads had appeared on a video posted by a white nationalist channel entitled “Wife With A Purpose.”

“We have strong values-led guidelines in place and are working with YouTube to understand how this could have slipped through the guardrails. We take these matters very seriously and are working to rectify this immediately,” a spokesperson for Under Armour said.

According to Fortune, YouTube’s parent company, Google, had the potential to lose as much as USD$750 million in revenue from advertisers boycotting YouTube. **Several major companies, including Johnson and Johnson, PepsiCo and McDonald’s, had already pulled their ads from the site.**

[Read the rest of the article online to learn more]

Majority of large charities have experienced cyber attacks

https://www.thirdsector.co.uk/majority-large-charities-experienced-cyber-attacks-says-report/management/article/1463172

More than seven in 10 large charities have fallen victim to cyber attacks or breaches in the past year, new research from the Department for Digital, Culture, Media and Sport has found.

A report based on the research, the Cyber Security Breaches Survey 2018, found that **73 per cent of the charities with annual incomes of more than £5m that took part in the survey had fallen victim to cyber attacks or breaches over the past year.**

The report says that, despite the prevalence of cyber security breaches in the sector**, only 21 per cent of all charities have a cyber security policy in place, and only 8 per cent have an existing cyber security incident management process.**

But 53 per cent of charities in the research said that cyber security was a high priority for senior management, **with the average cyber security breach that leads to financial loss costing a charity £1,030.**

The report, which was also produced by Ipsos Mori and the University of Portsmouth, is based on a "random probability" telephone survey of 569 charities and 1,519 businesses between 9 October and 14 December 2017, as well as 50 in-depth interviews with organisations featured in the survey.

The report says that of the 44 per cent of charities in the research that said they held personal data electronically, 30 per cent said they had experienced a cyber security breach.

The research also found that only six in ten charities that had experienced cyber breaches had taken preventive action to prevent a re-occurrence.

Only 42 per cent of charities had sought any guidance or advice on cyber security, and 5 per cent of them recalled using government guidance on the subject.

Staff training on cyber security was also poor among charities, the research found, with only 15 per cent of respondents sending their staff to any form of internal or external cyber security training in the past year.

[Read the rest of the article online to learn more]

ISO blocks NSA's latest IoT encryption systems amid murky tales of backdoors and bullying

https://www.theregister.co.uk/2018/04/25/nsa_iot_encryption/

Two new encryption algorithms developed by the NSA have been rejected by an international standards body amid accusations of threatening behavior.

The "Simon" and "Speck" cryptographic tools were designed for secure data to and from the next generation of internet-of-things gizmos and sensors, and were intended to become a global standard.

But the pair of techniques were formally rejected earlier this week by the International Organization of Standards (ISO) amid concerns that they contained a backdoor that would allow US spies to break the encryption. The process was also marred by complaints from encryption experts of threatening behavior from American snoops.

The ISO's meetings are confidential and held behind closed doors, but a number of encryption experts have broken their silence now that the NSA's three-year effort to push has effectively been ended.

"I worked very hard for this in the last year and a half. Now I can finally tell my story," tweeted one of the experts, Dr Tomer Ashur, who was representing the Belgian delegation.

He then pointed to the NSA's "outrageously adversarial" behavior during the process as a main reason why the two standards were rejected.

When some of the design choices made by the NSA were questioned by experts, Ashur states, the g-men's response was to personally attack the questioners, which included himself, Orr Dunkelman and Daniel Bernstein, who represented the Israeli and German delegations respectively.

Ashur further alleged that the NSA had plied the relevant ISO committee with "half-truths and full lies" in response to concerns, and said that if the American delegation had been "more trustworthy, or at least more cooperative, different alliances would have probably been formed."

Instead, he says, "they chose to try to bully their way into the standards which almost worked but eventually backfired."

[Read the rest of the article online to learn more]

More than 1 million kids had their identities stolen in 2017

https://nypost.com/2018/04/24/more-than-1-million-kids-had-their-identities-stolen-in-2017/

Your children may be less safe online than you think — even before they ever use a computer.

More than 1 million children were victims of identity fraud in 2017, a new study from Javelin Strategy & Research found, costing a total of $2.6 billion. With limited financial history or existing account activity, children are the most likely to become victims of new-account fraud, the research showed.

These attacks can occur before children even become active internet users, with some two-thirds of victims being under the age of 8. The overall numbers are likely even higher, said Al Pascual,

research director at Javelin, since the study relied on parents and guardians reporting cases of identity theft.

In many cases**, the parent or another relative may be the one using a child's identity to start a new account.**

Perhaps the most unnerving detail in the report: **The most common perpetrator of childhood identity theft is a family friend, accounting for 33 percent of the incidents.**

"If I am a parent and the lights have gone out, and I'm having a hard time making ends meet, using my child's identity to start a new account with the utility company may seem worth it," Pascual said. "I am doing right by them and not hurting them."

Other times, identities are compromised before they are even issued to children. **Michelle Dennedy, chief privacy officer of Cisco, became an advocate for child identity-theft prevention after her daughter was a victim of identity theft at the age of 8.**

Sometimes people do not know their identity has been compromised until they enter adulthood and apply for college, a car or a home, only to realize their credit has already been wrecked.

"Absolutely be as vigilant about your child's online reputation before they touch a device as you would about any other financial vehicle in your family because it can destroy families," she said. It can impact a child's ability to get a college scholarship and could lead to a long line of debt collectors, she added.

[Read the rest of the article online to learn more]

And Now this:

China using water spray, facial recognition technology to stop jaywalkers

https://globalnews.ca/news/4169368/china-jaywalkers-water/

In some of China's big cities, high-tech efforts are underway to stop pedestrians from jaywalking, state media reported on Thursday.

In central Hubei province, yellow posts equipped with lasers and motion-sensors were seen on curbs, CCTV reported, adding that **people will get sprayed by water if they attempt to cross on a red light.**

From April 23, **the southern city of Shenzhen launched 40 units of the "electronic police" — cameras with artificial intelligence that can identify jaywalkers automatically.**

CCTV also showed a big screen in Beijing that tells passersby that a nearby camera is monitoring and a loudspeaker will warn pedestrians who violate road rules and will ask them to go back to the stop line.

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
http://gov.bc.ca/informationsecurity
OCIOSecurity@gov.bc.ca

****