BRITISH COLUMBIA OCIO Office of the Chief Information Officer

Security News Digest

April 3, 2018

April is Spring Cleaning Month

Take our quiz and test your knowledge

On this day in history (April 3rd)

2009 – The first urban treaty in BC comes into effect as the Tsawwassen First Nation officially becomes self-governing.

This week's stories:

Saks, Lord & Taylor hacked; 5 million payment cards compromised 🇨🇦

Canadian Small Businesses 'Woefully Outgunned' in Battle with Cybercrime: Experts 🇨🇦

Atlanta Ransomware Attack Still Causing Chaos

Grindr is Sending All Kinds of User Data to Third-party Companies

Iranian hackers attacked college professors, US agencies and companies: Justice Department

The Ethical Minefield of 'Mind Reading' by Recording Brain Activity

Saks, Lord & Taylor hacked; 5 million payment cards compromised 🇨🇦

https://www.csoonline.com/article/3267573/security/saks-lord-taylor-hacked-5-million-payment-cards-compromised.html

Hackers made off with a whopping **5 million credit and debit card numbers** from Saks Fifth Avenue, Saks Off 5th, and Lord & Taylor, placing it "among the most significant credit card heists in modern history."

Parent company Canada-based Hudson's Bay Company announced the breach affecting the North American stores on Sunday, saying, "HBC has identified the issue, and has taken steps to contain it."

HBC disclosed the hack after cybersecurity firm Gemini Advisory revealed that the JokerStash hacking group, aka Fin7, claimed to have 5 million stolen payment card numbers the group intends to sell on the dark web. **The group responsible for this hack was also reportedly responsible for hacking "Whole Foods, Chipotle, Omni Hotels & Resorts, Trump Hotels and many more."**

Gemini believes the hackers [hacked] the retailers' point-of-sale systems and stole the card numbers between May 2017 and March 2018 from Saks Fifth Avenue, Saks Off 5th, and Lord & Taylor. The hackers likely got malware to infect the systems via phishing emails and then managed to steal the more than 5 million records by quietly sitting on the network for nearly a year.

Gemini added, "It appears that all Lord & Taylor and 83 U.S.-based Saks Fifth Avenue locations have been compromised. In addition, we identified three potentially compromised stores located in Ontario, Canada. However, the majority of stolen credit cards were obtained from New York and New Jersey locations."

On Wednesday, JokerStash announced a "brand new breach" called "BIGBADABOOM-2." The payment record details are being sold in small batches, so banks will have a harder time detecting the stolen card data. The hackers put a small number of compromised records up for immediate sale on the dark web. Of the 125,000 records for sale, Gemini said “approximately 35,000 records” are from Saks Fifth Avenue and “90,000 records” are from Lord & Taylor.

Although HBC promised that affected customers won’t be liable for fraudulent charges, Gemini pointed out that **“cardholders who frequently shop at luxury retail chains like Saks Fifth Avenue are more likely to purchase high-ticket items regularly; therefore, it will be extremely difficult to distinguish fraudulent transactions from those of a legitimate nature**, allowing criminals to abuse stolen payment cards and remain undetected for a longer period of time.”

In addition to the announcement on the Hudson’s Bay Company site, HBC also posted online notices on Saks Fifth Avenue, Saks Off 5th, and Lord & Taylor, saying the issue was identified and contained so that **“it no longer poses a risk to customers shopping at our stores. While the investigation is ongoing, there is no indication that this affects our e-commerce or other digital platforms, Hudson’s Bay, Home Outfitters, or HBC Europe. We deeply regret any inconvenience or concern this may cause.”**

HBC is reportedly working with data security investigators, as well as law enforcement and payment card companies. The company will offer impacted victims free identity protection services.

Canadian Small Businesses ‘Woefully Outgunned’ in Battle with Cybercrime: Experts 🇨🇦

https://globalnews.ca/news/4098752/canadian-businesses-outgunned-cybercrime/

Almost a third of Canadian businesses unknowingly divulged sensitive information — including customer data — to phishing scams in 2017.

According to the first Canadian Internet Security Survey conducted by the Canadian Internet Registration Authority (CIRA), this can be traced to a large gap between cybersecurity awareness and personal protection.

“Cybersecurity, whether it be for your home, your business or your corporation, is a prominent subject across all sectors … but the education associated with that is not a one-stop shop. It’s a long, complex process,” said Dave Chiswell, VP of product development at CIRA said in an interview.

While all businesses face cybersecurity challenges as attacks grow more sophisticated, small businesses without the resources to invest in expensive precautions often leave themselves vulnerable to these attacks, Chiswell said.

The report states that 77 per cent of small businesses that own their own domain are concerned about becoming the victim of cybercrime, but 36 per cent of respondents surveyed are not currently investing any money in protecting against cybercrime.

“The vast majority of internet users are uneducated, so there’s lots of low-hanging fruit for bad people on the internet,” Chiswell explained.

According to the general manager of Symantec Canada, Ajay K. Sood, small businesses and individual consumers are “woefully outgunned” when it comes preventing online security breaches.

“It’s not a question of whether you can be breached, it’s a question of whether you’re interesting enough to be breached,” said Sood.

Sood adds that the growing complexity of cybercrime makes preventing these attacks especially difficult for small businesses with limited resources. The simplest attacks, such as email phishing scams, can have devastating consequences for small business owners and consumers who don’t know how to recognize them.

“Phishing is low tech, it’s just sending an email. But it’s also high crime,” Sood explained.

The CIRA report also goes on to state that awareness about cybercrime is growing, but this hasn’t been accompanied by a decrease in attacks as one might expect. Sood explained why increasing awareness is actually likely to be followed by an uptick in successful attacks.

“At the end of the day, as awareness grows of attacks and cybercriminals, the attack surface is also growing. The more people coming into technology, the greater attack surface you have,” he said.

While it’s become increasingly difficult to prevent a cyber attack, both Chiswell and Sood have suggestions for small business owners looking to increase their security.

Chiswell advised business owners to sign up with a security provider that's well known and trusted. Sood on other hand urged Canadians to train themselves to recognize at least a handful of potential attacks.

For example, Sood explained that phishing emails usually promise users some extreme benefit for opening their email, such as a large sum of money or other reward, and warn of a detrimental consequence for ignoring it.

"Cyber has to be considered a general threat. What I'm really talking about is a culture change," said Sood.

Atlanta Ransomware Still Causing Chaos

https://www.cbsnews.com/news/atlanta-ransomware-attack-still-causing-chaos/

Computers were turned back on Tuesday in Atlanta, but that doesn't mean it's back to business as usual.

Five days after a "ransomware" attack crippled the city's computer network, officials are trying to recover from the hack that blocked access to electronic records, leaving city jails and municipal courts running manually with paper and pens. Many city employees remain without access to email or the internet.

Atlanta's courts also said they are are unable to process ticket payments because of the breach, whether online or in person. Residents facing court cases for some low-level offenses received a reprieve of sorts due to the attack.

The use of ransomware, which lets hackers seize control of computers belonging to individuals, businesses and local governments, has been on the rise in recent years. In 2017, U.S. officials blamed North Korea for the massive "WannaCry" ransomware attack on hospitals, financial firms and other companies.

More than 1,200 ransomware incidents were detected every day last year, according to a new report from security software firm Symantec.

Investigators including the Federal Bureau of Investigation are working to figure out the identity of the culprits, who demanded the equivalent of about $51,000 in bitcoin to unlock the shuttered systems.

Atlanta Mayor Keisha Lance Bottoms declined to indicate if city officials are considering paying the ransom, saying in a televised news conference on Monday that she is consulting with the FBI and other federal agencies.

"We are dealing with a hostage situation," Bottoms said in declining to specify when the city expects to be fully operational again.

"There's a lot of work that needs to be done with our digital infrastructure in the city of Atlanta, and we know that year after year that it's something that we have to focus on, and certainly this has speed things up," Bottoms said.

"For some of our younger employees, it will be an exercise in good penmanship," she quipped in a light-hearted moment talking about the situation that has city employees performing tasks manually instead of electronically.

On Tuesday, the city advised employees to turn on computers and printers for the first time since the attack, while warning in a statement that some systems may still be down.

Secureworks, an Atlanta security firm hired by the city to help it resolve its online issues, declined in an email to comment the incident.

The impact of the cyberattack is still affecting Hartsfield-Jackson Atlanta International Airport, which shut down its WiFi system as a precaution. A notice on the website of the world's busiest airport said internet difficulties meant security wait times and flight information were unavailable, and advised travelers to check with individual airlines.

Beyond Atlanta, a suburban town 30 miles away is advising residents to monitor their bank accounts and credit report because a hacker may have gained access to a city server in Loganville, Georgia. The possible hacking occurred on March 15, and personal and financial information including Social Security numbers and banking information may have been compromised, the city announced Monday on Facebook.

Grindr is Sending All Kinds of User Data to Third-party Companies

https://mashable.com/2018/04/02/grindr-user-privacy-hiv-status/

Grindr has a communication problem.

The social networking app used by 3.6 million people has been doing more than simply facilitating hookups, and in the process has potentially put the privacy of its users at risk.

According a report from BuzzFeed News, the company is sharing user data with two other companies — data that includes email addresses, **GPS data, phone IDs, and HIV statuses. Taken as a whole, this information could be used to determine the HIV status of individuals by name.**

After all, how many of you use some form of your real name as your email address? This, paired with your phone ID and GPS location, is likely more than enough to peg data to a specific person. What's more, even if Grindr doesn't have specific health data on you, this information might be enough to identify you as a user of a queer-focused app.

The companies in question are Localytics and Apptimize. Apptimize bills its service as helping companies "make better apps," and Localytics says its goal is "to help customers build stronger relationships with their mobile and web app users through our analytics and marketing platform."

So why do they need to know Grindr users' self-reported HIV statuses? According to Grindr, it's to make the app better.

"As an industry standard practice, Grindr does work with highly-regarded vendors to test and optimize how we roll out our platform," a company spokesperson told Mashable over email. "These vendors are under strict contractual terms that provide for the highest level of confidentiality, data security, and user privacy."

The statement further noted that yes, the "data may include location data or data from HIV status fields as these are features within Grindr, however, this information is always transmitted securely with encryption, and there are data retention policies in place to further protect our users' privacy from disclosure."

And while the spokesperson insisted in the statement that "Grindr has never, nor will we ever sell personally identifiable user information – especially information regarding HIV status or last test date – to third parties or advertisers," that doesn't apply here as no one has accused Grindr of selling this information.

Following BuzzFeed News's report, Bryan Dunn, VP of Product at Localytics, issued a statement clarifying his company's policy surrounding the data it receives.

"We do not share, or disclose, our customer’s data," read the statement in part.

Still, this is all obviously not a good look for Grindr. The move to share HIV status information with other companies potentially puts the health and safety of users at risk. If that data were to leak or be stolen, or even accessed inappropriately by someone at Apptimize or Localytics, it could be devastating for those whose privacy was violated as a result.

Just exactly how devastating is revealed by a current lawsuit against CVS for allegedly unintentionally revealing the HVS status of 6,000 customers in Ohio. In that case, individuals claim to have experienced significant emotional distress following their nonconsensual exposure.

Grindr's sharing of this immensely personal data with other companies, no matter the stated intention and protections put in place, could have similar consequences if things went wrong. And on the internet, things almost always go wrong eventually.

UPDATE: April 2, 2018, 3:53 p.m. PDT According to Axios, Grindr will stop sharing the HIV status of its users with third-party companies.

Iranian hackers attacked college professors, US agencies and companies: Justice Department

https://www.cnbc.com/2018/03/23/us-indicts-iranian-nationals-in-iran-government-backed-scheme-on-us-universities.html

Nine Iranians were charged Friday by the Justice Department in a wide-ranging scheme to hack and steal electronic data from universities, private corporations and U.S. government entities to benefit the government of Iran.

The Iranians were indicted on seven counts accusing them of identity theft and conspiracy to commit computer intrusions.

The nine allegedly accessed the computer systems of U.S. universities through duplicitous electronic contacts, a scheme known as phishing. They targeted more than 100,000 professor email accounts at 144 American universities through the spearphishing campaign, the indictment said.

The activity, which had allegedly been conducted since 2013, could cost universities $3.4 billion.

"That type of criminal activity does not just cause economic harm," Deputy Attorney General Rod Rosenstein said. "It also threatens our national security. Identifying and prosecuting computer hackers is a priority for the Department of Justice."

The nine defendants were accused of being affiliated with the so-called Mabna Institute and acted at the behest of one of Iran's intelligence gathering entities.

They also targeted and compromised at least 36 U.S.-based private companies and at least 11 companies based in Germany, Italy, Switzerland, Sweden and the United Kingdom, proescutors said.

And the indictment counts at least five government agencies, including the Labor Department, the Federal Energy Regulatory Commission and the United Nations, among the victims of the hacking campaign.

The nine are at large, the Justice Department said.

In addition to the hacks on U.S. entities, accounts from 176 universities outside the U.S. were targeted, authorities said.

The data breaches successfully compromised roughly 7,998 accounts or more worldwide, and at least 3,768 belonged to professors at U.S. universities, investigators said.

"Academic institutions are prime targets for foreign cybercriminals. Universities can thrive as marketplaces of ideas and engines of research and development only if their work is protected from theft," Rosenstein said.

The Treasury Department's Office of Foreign Assets Control issued sanctions against the Iranians on Friday.

Rosenstein announced the indictments alongside several senior officials — including David Bowdich, who succeeded Andrew McCabe as the FBI's acting deputy director following McCabe's firing last week.

And Now this:

The Ethical Minefield of 'Mind Reading' by Recording Brain Activity

http://www.cbc.ca/news/health/eeg-mind-reading-ethics-1.4596685

In a small room tucked away at the University of Toronto, Professor Dan Nemrodov is pulling thoughts right out of people's brains.

He straps a hat with electrodes on someone's head and then shows them pictures of faces. By reading brain activity with an electroencephalography (EEG) machine, he's then able to reconstruct faces with almost perfect accuracy.

Student participants wearing the cap look at a collection of faces for two hours. At the same time, the EEG software recognizes patterns relating to certain facial features found in the photos. Machine-learning algorithms are then used to recreate the images based on the EEG data, in some cases within 98-per-cent accuracy.

Nemrodov and his colleague, Professor Adrian Nestor say this is a big thing.

"Ultimately we are involved in a form of mind reading," he says.

The technology has huge ramifications for medicine, law, government and business. But the ethical questions are just as huge. Here are some key questions:

What can be the benefits of this research?

If developed, it can help patients with serious neurological damage. People who are incapacitated to the point that they cannot express themselves or ask a question.

According to clinical ethicist Prof. Kerry Bowman and his students at the University of Toronto, this technology can get inside someone's mind and provide a link of communication. It may give that person a chance to exercise their autonomy, especially in regard to informed consent to either continue treatment

In a courtroom, it may end up being used to acquit or convict those accused of crime. Like lie detector tests and DNA analysis, brain scanning our memories may become a legal tool to help prove innocence or guilt.

It may even change our relationship with animals. If, as student Nipa Chauhan points out, we know what they understand and feel, we may act differently toward them.

So what's the flipside? A lot.

Let's start with the concept of memory. Our memories are never "pure" — nor are they ever complete.

And our brain often fills in the blank spots with biases and personal reflections. Researchers like Adrian Nestor and his colleague Dan Nemrodov agree it's still a bit like archaeology-digging beneath the layers to find the raw information. They haven't found it yet, but they believe it's just a matter of time.

That, according to Bowman and his students, raises the thorny issue of freedom, especially freedom of thought.

"Nobody can tell me what to think or when to think or how to think. This is the first time that freedom can be infringed upon," says Bowman.

And from there it can take unpredictable turns. Could a person be compelled to undergo mind reading in order to apply for a job or to gather evidence for police? Would it ever be ethically acceptable to allow this without consent?

"How might we regulate that, especially since it's ripe for abuse with authoritarian regimes? Without consent to do that would be very problematic," says student Yusef Manialawy.

[Read the rest of the article online to learn more about this story]

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:
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

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.

****