Security News Digest
March 21, 2017

- March is Fraud Prevention Month -
Take the Top Ten Scams Quiz

Visit the Information Security Branch Fraud Prevention Month Page:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-awareness/fraud-prevention-month

TODAY: Shoppers Drug Mart Computer Crash Causes Customer Confusion and Frustration
http://www.cbc.ca/news/business/shoppers-drug-mart-computer-crash-1.4034194

Nationwide glitch is affecting both prescriptions and transactions at stores – Last updated at noon today.

An intermittent computer system outage is hampering business at Shoppers Drug Mart stores across the country. CBC News confirmed the problem with the drug store giant after receiving complaints from customers that they were having difficulty making purchases or getting their prescriptions filled. *Shoppers said that the computer glitch is hampering electronic payments. That means customers can't use their debit cards and won't receive any Optimum points on purchases today at affected stores.*

…Yesterday at about 4:30 p.m., Smith went to her local Shoppers to get a prescription filled and returned home empty-handed. She said she was the eighth person in line and that the pharmacist was telling everyone that they wouldn't be getting their drugs anytime soon. ..*Shoppers operates more than 1,300 drug stores across Canada*. Earlier today, Smitham [of Shopper's] said that it's IT team is "working diligently" to fix the computer glitch. [apparently, it was a computer upgrade that did not work properly]

Money Laundering Watchdog Scrutinizes Facebook, Social Media
http://www.cbc.ca/news/politics/facebook-twitter-privacy-moneylaundering-1.4020638

Canadians who make large cash transactions, international wire transfers or win big at the casino could end up with a federal agency scrutinizing their Facebook pages and other social media posts, CBC News has learned. The Financial Transactions and Reports Analysis Centre (FINTRAC), the federal government body charged with monitoring financial transactions to detect money laundering and terrorist financing, has been quietly scrutinizing the social media posts of Canadians whose transactions attract its attention. FINTRAC defends the practice, saying the rules that govern it allow it to collect a variety of information. "FINTRAC's mandate is to detect, deter and prevent money laundering and terrorist financing activity," spokesperson Renée Bercier wrote in response to questions from CBC News. "It is important to remember that the perpetrators of these crimes oftentimes have an online presence and actively use the web, including social media, to connect with associates, facilitate their activities and, in the case of terrorism financing, even raise funds."

Privacy concerns raised However, privacy advocates and NDP MP Daniel Blaikie say that just because something is publicly available doesn't mean that it's fair game for government bodies to scrutinize or monitor. One of the things about social media right now is it's kind of the Wild West, because the technology has moved a lot faster than regulation and a lot of Canadians may not realize that their social media account is being used and viewed in this way," said Blaikie. "So, it does make sense to have a look at that and to ask whether or not there ought to be rules around how government uses information that's available on people's social media accounts." Blaikie wants Parliament's access to information, privacy and ethics committee to examine the question and hear from experts on what kinds of regulations the government should adopt.

Taxman monitors Facebook In January, CBC News revealed the Canada Revenue Agency has been scrutinizing the Facebook pages and other social media posts of Canadians who it suspects could be

cheating on their taxes. CBC News has since learned that the Canadian Anti-Fraud Centre has also filed a privacy impact assessment with Privacy Commissioner Daniel Therrien's office, listing social media posts as one of the things it checks when looking into complaints of fraud and scams.
….Bercier said the Proceeds of Crime (Money Laundering) and Terrorist Financing Act gives FINTRAC the authority to collect publicly available information, including information from commercial databases, to sign agreements to access databases maintained by federal, provincial or foreign governments and to receive information provided voluntarily by law enforcement, intelligence agencies, security commissions, foreign financial intelligence units and the general public.
Accidental sharing David Christopher, spokesperson for Open Media, said there is cause for concern, particularly given the complexity of Facebook's privacy settings, which often lead to people accidentally posting something publicly. .."When people are posting on social media, especially when they are sharing on Facebook, they mostly believe that they are sharing with friends and family - not with the government, not with total strangers."

Man Accused of Extortion of Amanda Todd Sentenced to Jail in Netherlands

http://www.cbc.ca/news/canada/british-columbia/man-accused-of-extortion-of-amanda-todd-sentenced-to-jail-in-netherlands-1.4027293
The Dutch man accused of cyber-bullying Port Coquitlam, B.C., teen Amanda Todd has been sentenced to 10 years and 8 months in prison, in an unrelated but high-profile trial in the Netherlands. Aydin Coban, 38, was given the sentence by a court in Amsterdam Thursday morning, *on charges related to the abuse of 34 young girls and five men*. A court summary shows that Coban was also accused of blackmail, co-perpetration of rape, attempted rape and seduction charges as well as several other child pornography-related offences. According to the Dutch prosecution office, Coban's victims lived in countries including the Netherlands, Australia, Norway, the U.K. and United States.
Coban is facing five separate charges in Canada in relation to Amanda Todd, including possession of child pornography and extortion. He's set to be extradited after the proceedings in the Netherlands conclude, although he's filed legal appeals to stay in his home country.
In October 2012, Amanda Todd, *a 15-year-old from Port Coquitlam, committed suicide after posting a video on YouTube saying she was blackmailed by an online predator after exposing her breasts on a webcam*. Her mother Carol Todd was anxious for the verdict. While her daughter's case isn't part of the European proceedings, Todd travelled to the Netherlands to be in the courtroom when the trial first started. .."The verdict will have influence on the world and everyone who has been following these types of stories, the future acts we see, the future investigations, and trials that we hope will come out of it," said Todd.

Central Huron Health Records Snooping Case Prosecuted

http://blackburnnews.com/midwestern-ontario/2017/03/16/central-huron-health-records-snooping-case-prosecuted/
Ontario - *A Justice of the Peace in Goderich has handed down the stiffest fine to date in Canada for a health privacy breach*. A university student who was on an educational placement with the family health team in Central Huron has been ordered to pay a $20,000 fine and a $5,000 victim surcharge for accessing personal health information without authorization. The student pled guilty to willfully accessing the personal health information of five individuals. As part of her plea, she agreed that she accessed the personal health information of 139 individuals without authorization between September 9th, 2014 and March 5th, 2015.
In March 2015, *the Information and Privacy Commissioner was advised that the individual was found to have been illegally accessing the records of family, friends, local politicians, staff of the clinic and other individuals in the community*. The matter was turned over to the Attorney General for prosecution. In delivering her reasons for sentence, the Justice of the Peace stated that: “Overall, the victim impact statements reveal a lack of trust and a sense of reluctance to share information with future health care providers. I believe this is a truly significant factor, given that *we all must believe that when we go to the doctor for our physical illnesses and our mental health illnesses, that we will be able to trust our own health care practitioners and their team and that what we tell them will be respected and held in confidence so we receive the treatment and care we deserve*.”

Facial Recognition Coming in for a Landing at Ottawa Airport Today [March 20]

http://www.cbc.ca/news/canada/ottawa/kiosk-airport-cbsa-app-1.4031840

It's a sure sign that your vacation is coming to an end. That moment when the flight attendant walks down the aisle of the plane, handing out declaration forms, as passengers scramble to find a pen. But the days of the paper form are numbered.
Starting Monday, passengers arriving on international flights to the Ottawa airport are encouraged to use a self-serve kiosk, called a primary inspection kiosk, to speed up and streamline the arrival process. To verify a traveller's identity, the new kiosks will a take a photo and compare it to their passport picture.
Travellers can either complete an on-screen declaration at the kiosk, or use the newly launched mobile app. Once downloaded, travellers can use it in airplane mode, allowing them to fill it out before they land. They'd then scan their phone at a kiosk before continuing on to baggage claim. NEXUS members will not be able to use the app, but still continue to use the NEXUS kiosks.
….But Customs and Immigration Union president Jean-Pierre Fortin, who represents 10,000 frontline customs and border agents, *wonders why, in 2017, the government is taking humans out of the equation. He says his officers get 18 weeks of intensive training. "They're looking for tons of things: your attitude in general, are you nervous...It's a bunch of factors that machines will never be able to detect,"* he said. "They develop these skills actually to make sure that they're stopping the people that they think there's something wrong with."
On its website, the border agency says the kiosks are secure and only store non-sensitive information. But that's not enough for everyone. Ian Kerr, Canada research chair in ethics, technology and law at the University of Ottawa, told CBC Radio's *All in a Day* the kiosks could be outfitted with sensors that function like a lie detector or be programmed with algorithms to assess whether a traveller is a potential risk. "We have to think really carefully before we implement [technologies like this] because they can ultimately be used for things beyond the purposes that they started being used," Kerr said. The CBSA was not available for an interview Sunday.

New Rules for Flying Recreational Drones in Canada Revealed

http://www.cbc.ca/news/politics/canada-drone-regulations-marc-garneau-1.4027486
Recreational drone users in Canada face new restrictions on where and when they can fly their remote-controlled devices, under new rules being announced today by Transportation Minister Marc Garneau.
The rules, which are effective immediately, mean recreational users will face a fine of up to $3,000 if drones weighing more than 250 grams are caught flying: Higher than 90 metres, Within 75 metres of buildings, vehicles, vessels, animals or people, More than 500 metres away from the user, At night, in clouds or somewhere you can't see it, Within nine kilometres of somewhere aircraft take off or land, or a forest fire, Without your name, address and phone number marked on the drone itself, and Over forest fires, emergency response scenes or controlled airspace.
Some of those rules existed only as guidelines before the announcement, Garneau said, with no specific penalties for breaking them. RCMP Chief Supt. Brian Stubbs said at the announcement at Toronto's downtown Billy Bishop Airport that police could really only penalize someone using a drone dangerously if they broke a section of the Criminal Code, such as criminal negligence or mischief. "These regulations will give us a [less harsh] way to manage these types of calls," he said. "Of course discretion is a part of this as well too. Police officers have the discretion just to educate, perhaps, an operator of a drone, all the way to [using] the Criminal Code." Transport Canada says anyone who sees someone flying a drone illegally should call 911.
The new rules do not apply to people flying at sites and events sanctioned by the Model Aeronautics Association of Canada, a national model aircraft association Garneau said has an excellent safety record. Garneau pointed out that people who use drones for commercial, academic or research reasons already have to get a special certificate, and most fly them safely. But he added that Transport Canada has noticed a large increase in the number of reported safety incidents involving drones in the last three years: 41 in 2014, 85 in 2015 and 148 last year. "I believe that we have to strike the right balance between encouraging the drone industry, but doing it responsibly," he said.

Why Top ISPs Don't Think Your Web History or App Usage is 'Sensitive Information'

http://www.techrepublic.com/article/why-top-isps-dont-think-your-web-history-or-app-usage-is-sensitive-information/
Internet service providers (ISPs) said that web browsing and app usage history should not be considered "sensitive information," according to a recent filing with the Federal Communications Commission (FCC). The CTIA, an advocacy group representing ISPs including AT&T, Verizon Wireless, T-Mobile USA, and Sprint, filed a document with the FCC on March 16, stating that that group's consumer privacy rules

passed during the Obama administration should be rolled back. *The privacy rules require ISPs to obtain consent from consumers to use and share sensitive information*, including web browsing history, app usage history, and the content of communications, as well as geolocation, financial information, health information, children's information, and social security numbers. The Obama era opt-in rules are scheduled to take effect on December 4, 2017. *If ISPs win their petition to the FCC to eliminate the rules, the ISPs could potentially sell web and app usage history to advertisers*. The CTIA based its argument that web browsing and app usage history should not be considered sensitive information on differences between the FCC's position and that of the Federal Trade Commission (FTC).

EU Authorities Demand Changes from Facebook, Google, Twitter

http://www.theglobeandmail.com/technology/eu-authorities-demand-changes-from-facebook-google-twitter/article34335812/

Social media companies Facebook Inc, Alphabet Inc and Twitter Inc will have to amend their terms of service for European users within a month or face the risk of fines, a European Commission official said on Friday. U.S. technology companies have faced tight scrutiny in Europe for the way they do business, from privacy to how quickly they remove illegal or threatening content. The Commission and European consumer protection authorities will “take action to make sure social media companies comply with EU consumer rules,” the official said. The comments confirmed a Reuters report from Thursday.

Germany, the most populous EU state, said this week it planned a new law calling for social networks such as Facebook to remove slanderous or threatening online postings quickly or face fines of up to €50-million ($53-million). The authorities and the Commission sent letters to the companies in December saying that some of their service terms broke EU consumer protection law and that they needed to do more to tackle fraud and scams on their websites. The companies proposed some ways to resolve the issues and discussed them with the authorities and the Commission on Thursday, a source familiar with the matter said, adding that the meeting was constructive. According to the letters seen by Reuters, some of those contested terms include requiring users to seek redress in court in California, where the companies are based, instead of their country of residence.

Other issues include not identifying sponsored content clearly, requiring consumers to waive mandatory rights such as the right to cancel a contract, and an excessive power for the companies to determine the suitability of content generated by users, according to the letters. In the case of Alphabet’s Google unit, the concerns were about its social network Google+. Google and Facebook were not immediately available for comment. A spokesman for Twitter declined to comment.

Internet of Things Security: What Happens When Every Device is Smart and You Don't Even Know It?

http://www.zdnet.com/article/internet-of-things-security-what-happens-when-every-device-is-smart-and-you-dont-even-know-it/

Billions more everyday items are set to be connected to the internet in the next few years, especially as chips get cheaper and cheaper to produce - and crucially, small enough to fit into even the smallest product. *Potentially, any standard household item could become connected to the internet, even if there's no reason for the manufacturers to do so*. *Eventually the processors needed to power an IoT device will become effectively free, making it possible to turn anything into an internet-enabled device*. "The price of turning a dumb device into a smart device will be 10 cents," says Mikko Hyppönen, chief research officer at F-Secure. *However, it's unlikely that the consumer will be the one who gains the biggest benefits from every device in their homes collecting data; it's those who build them who will reap the greatest rewards - alongside government surveillance services*. "It's going to be so cheap that vendors will put the chip in any device, even if the benefits are only very small. But those benefits won't be benefits to you, the consumer, *they'll be benefits for the manufacturers because they want to collect analytics*," says Hyppönen, speaking at Cloud Expo Europe.

For example, a kitchen appliance manufacturer might collect data and use it for everything from seeing how often the product breaks to working out where customers live and altering their advertising accordingly in an effort to boost sales - and the user might not even know this is happening, if devices have their own 5G connection and wouldn't even need access to a home Wi-Fi network. *"The IoT devices of the future won't go online to benefit you - you won't even know that it's an IoT device," says Hyppönen. "And you won't be able to avoid this, you won't be able to buy devices which aren't IoT devices, you won't be able to restrict access to the internet because they won't be going online through*

your Wi-Fi. We can't avoid it, it's going to happen." Indeed, it's already started, with devices you wouldn't expect to need an internet connection - including children's toys - being discovered to have gaping cybersecurity vulnerabilities.
These scenarios, says Darren Thomson, CTO & vice president of technology services at Symantec, are occurring because those in the technology industry are thinking about whether they could connect things to the internet, but aren't thinking about whether they should. "Could I attach my dog to the internet? [note: there already are 'fitness trackers' for dogs and for cats, e.g. FitBark] Could I automate the process of ordering a taxi on my mobile phone? We're obsessed with 'could we' problems. That's how we live our lives and careers, we invent things and we solve problems. We're good at 'Could we'," he said, also speaking at Cloud Expo Europe. *No matter the reason why things are being connected to the internet, Thomson agrees with Hyppönen about what the end goal is: data collection*. …However, various incidents have demonstrated how *the Internet of Things is ripe with security vulnerabilities as vendors put profit and speed to market before anything else, with cybersecurity very low down the list of priorities*. Retrofitting updates via the use of patches might work for a PC, a laptop or even a smartphone, but there are huge swathes of devices - and even whole internet-connected industrial or urban facilities - for which being shut down in order to install and update is impossible.
...Not only that, but as IoT devices become more and more common, people will start to ignore them. "The reality of the human mind is as we embed things, we tend to forget about them, we get complacent about them. ..Even now, consumers are too blasé about connected devices, keen to jump on the latest technological trends failing to realise the associated security risks. Then even if they do, they remain unclear on how to secure the IoT devices - that is, if there is the option of securing it in the first place. ..He likens it to the "exact same problem we had in the 80s" when people wouldn't even bother to set a time on their video recorder as it involved picking up the manual, so it'd end up always flashing 12:00.
…But are IoT device manufacturers going to do this anytime soon? Probably not. "The manufacturers of IoT devices are unlikely to fix this by themselves. They're unlikely to start investing more money in their IoT devices for security because money is the most important thing in home appliances," says Hyppönen. *..It might eventually be regulation which has to fix this problem; as Hyppönen points out, device safety is already regulated. "When you buy a washing machine, it must not short circuit and catch fire, we regulate that. Maybe we should regulate security," he says*.

Russian Hacker "Kolypto" Who Worked on Citadel Trojan Extradited to the US

https://www.bleepingcomputer.com/news/security/russian-hacker-kolypto-who-worked-on-citadel-trojan-extradited-to-the-us/

On March 14, a Russian national accused of helping develop the Citadel banking trojan was arraigned in front of a US judge for the first time, after being extradited from Fredrikstad, Norway. The man's name is Mark Vartanyan, 28, known online as Kolypto. According to US authorities, Vartanyan allegedly developed, improved and maintained the Citadel malware, a banking trojan made available via a Malware-as-a-Service offering. *The Citadel trojan came to the security industry's attention in 2011, and was initially based on the source code of the ZeuS banking trojan, which leaked online months before*. Citadel evolved over the years, under the supervision of Aquabox, the malware's creator. According to US authorities, Vartanyan is one of Aquabox's helpers. ..Previously, during Citadel's main domination period, between 2011 and 2012, Vartanyan lived in the Ukraine. Citadel's activity started to die down in December 2012, after its creator, Aquabox, took the trojan off the market. Initially, when authorities arrested Vartanyan, they thought they nabbed Aquabox. This turned out to be false, and Aquabox remains at large.

Russian authorities contesting extradition charges

Vartanyan fought his extradition for almost two years, before losing his case in December 2016. During this time, he was held under house arrest in Norway. Russia's ambassador to Norway contested the extradition proceedings. In February 2017, the Russian Ministry of Foreign Affairs said "Norway violated international law by approving the extradition of Russian citizen Mark Vartanyan to the US for trial." *This is not the first time Russian officials contest the extradition of Russian hackers to the US. Currently, Russia is putting pressure on the Czech Republic not to extradite Yevgeniy Nikulin, a hacker accused of breaching LinkedIn, Dropbox, and Formspring in 2012*.

Here's How the FBI Says Russian Hackers Stole Yahoo Account Secrets

http://www.cbc.ca/news/technology/russian-yahoo-hackers-indictment-500-million-emails-how-1.4029532

[NOTE: the entire story is given here, to create an awareness of how hackers operate. It is lengthy, so it is the final story in today's Security News Digest]

For more than two years, criminal hackers had control of Yahoo's most sensitive computer systems, giving them unprecedented access to more than 500 million user accounts - and Yahoo staff were none the wiser. The allegations, part of an FBI indictment against three Russians and a Canadian filed in a California court earlier this week, tell the story behind *one of the largest corporate data breaches ever committed*.

The tale begins in early 2014, when two Russian intelligence officers, Dmitry Dokuchaev and Igor Sushchin, sought access to potentially valuable email accounts - those belonging to U.S. and Russian government officials, but also Russian journalists, and employees of additional email and internet service providers.

They enlisted the help of two alleged criminal hackers to do so, each responsible for a different task. Alexsey Belan, *a Russian in the employ of Russia's Federal Security Service, or FSB*, found a way into Yahoo's servers. Once inside, Belan accessed systems that stored and managed account data. Importantly, those systems could be used to either reset or modify account security mechanisms, and in some cases, bypass a user's password altogether.

The indictment alleges that later that year, Russian intelligence officers separately turned to Karim Baratov, a 22-year-old Canadian hacker of Khazhak origin living in Ancaster, Ont., a suburb of Hamilton. After identifying Yahoo accounts of interest, Baratov was instructed to find other webmail accounts held by the targets - Google accounts, in particular - and break in. It's not clear what, exactly, tipped Yahoo staff off to the ongoing intrusion - though a hacker by the name of Peace, who claimed to be selling account credentials belonging to about 200 million Yahoo users on the dark web last August, may have had something to do with it. Whether Peace was telling the truth is hard to say, but within weeks, Yahoo confirmed that it had been breached.

To gain access to Yahoo's servers, the indictment suggests that the Russian hacker Belan employed a common attack known as spear phishing, in which otherwise malicious emails are made to look legitimate. *A spear phishing email might instruct a person to download and open an attachment, which secretly contains malware. Or it may direct the recipient to enter their username and password after clicking on a link to a website designed to look like the login page of, say, a legitimate Gmail account*.

The FBI alleges that Belan used spear phishing attacks to target Yahoo employees and steal their account credentials. He is said to have gained access to a Yahoo server in early 2014, and further access to the company's corporate network by September of that year.

Along the way, the attackers are said to have installed software that would cover their tracks - designed to scrub server logs, for example - making it harder for the Yahoo security team to notice they were there. By October, *they had obtained information about Yahoo's Account Management Tool, or AMT, which Yahoo administrators used to manage and modify information about accounts - user names, recovery email addresses and phone numbers, security questions and answers, and more*.

That information was stored in Yahoo's User Database, or UDB, and they obtained a backup copy by early November 2014, containing information for more than 500 million accounts - *gaining them access to the account of any user whose password had not been changed after that time*.

Minting cookies

Throughout 2015 and 2016, the attackers used their access to Yahoo's AMT and the information contained within the stolen UDB to target user accounts of interest. *One technique allowed the attackers to generate cookies - **files commonly used by websites to remember users, so they don't have to enter their password each time** — through a process called "cookie minting."* [security best practice tip – don't use "remember me" or "remember my password", as this is why..]

The cookies "allowed the conspirators to appear to Yahoo's servers as if the intruder had previously obtained valid access to the associated Yahoo user's account, obviating the need to enter a username and password for that account," the indictment says. At first, the attackers generated the cookies on Yahoo's servers. But by August 2015, they had obtained Yahoo's cookie minting code, which allowed them to go through the process on their own machines. *According to the indictment, the attackers used these cookies "to access the contents of more than 6,500 Yahoo user accounts."*

Along the way, it became clear to Dokuchaev and Sushchin, the Russian intelligence agents, that *some of their targets had other webmail accounts with different providers - which they directed the alleged Canadian hacker Baratov to access. Using the same techniques that Belan first used to gain access to Yahoo's infrastructure, Baratov is alleged to have launched a number of spear phishing attacks, gaining*

access to at least 80 email accounts, including at least 50 Google accounts. He was allegedly paid around $100 per account.

'Spam marketing scheme'

While all this was going on, *Belan, the criminal hacker who worked in the employ of Russian intelligence, is also alleged to have used his access to Yahoo accounts for personal gain - searching accounts for gift cards, credit card numbers, and login information for financial services such as PayPal. And it alleges that Belan also used minted cookies to steal contact information from 30 million Yahoo accounts "as part of a spam marketing scheme."*

Russian intelligence officials were only too happy to help Belan evade detection, according to the FBI. Last July, they sent him "information regarding FSB law enforcement and intelligence investigations, and FSB tactics, including its use of information to target hackers whose difficult-to-trace computer intrusion infrastructure made other means of surveillance more difficult." In fact, throughout the entire operation, the FBI alleges the attackers "attempted to hide the nature and origin of their internet traffic" so they would not be detected by their victims and law enforcement alike - *using servers in different countries, virtual private networks (VPNs), and multiple false email accounts*.

But all that appears to have come to an end, beginning last fall. The breach was disclosed publicly in September, and Yahoo began working with the FBI. And while the indictment says the attackers continued to use their stolen information, that too was short lived. Dokuchaev, one of the intelligence officers, was reportedly arrested in Russia, in December, on separate charges. Baratov, of course, is being held in custody, and U.S. officials are seeking his extradition to face charges in a California court. A bail hearing has been set for April 5. As for Sushchin and Belan, Russian officials have denied their government's involvement. There is no extradition treaty between Russia and the U.S., and their whereabouts remain unknown.

Feel free to forward the Digest to others that might be interested.
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 Technology, Innovation and 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.

****