BRITISH COLUMBIA OCIO | Office of the Chief Information Officer

Security News Digest
June 06, 2017

(sent on June 07, 2017)

Thursday, June 08 is the Information Security Branch
SECURITY DAY
The theme is “The Internet of Things: is your lightbulb spying on you?”
You are invited to go to this link to watch the free webcast:
http://video.web.gov.bc.ca/mtics/live/securityday.html

The pdf Agenda is available here: http://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-security/information-security-awareness/agenda_securityday_jun08_with_descriptions.pdf

And please, Enjoy our June 2017 Internet of Things Quiz!

Check Your Tickets: Air Canada Cancels Bookings Without Warning 🇨🇦

http://www.cbc.ca/news/canada/british-columbia/check-your-tickets-air-canada-cancels-bookings-without-warning-1.4147410

A number of Air Canada customers have had their tickets cancelled without warning - *the latest is a Vancouver woman who only learned her ticket had been refunded when she checked her credit card statement*. Nina Chung, 35, says *she received no notice from Air Canada*. Even more confusing, her booking on the airline's website still states the ticket is confirmed. But airline representatives have told Chung the site is wrong - she doesn't have a ticket. ..An air passenger rights advocate says the issue appears to stem from changes to Air Canada's fraud detection system, which is falsely flagging valid credit cards.

Gabor Lukacs said he has received "a number of complaints" from Air Canada passengers in recent weeks, all involving surprise cancellations of bookings. "There is no doubt there is something fundamentally wrong here with the system," said Lukacs. *"A fraud detection system that has so many false positives is obviously faulty."* Air Canada spokesperson Angela Mah refused to say if there has been a spike in false flagging of credit card transactions, *but confirmed the airline's online security system has been undergoing changes*. "We're optimizing our anomaly detection and prevention tools and security systems constantly, as credit card fraud costs everyone," Mah wrote in an email to CBC News. …*A CBC News investigation, however, shows a pattern: Credit card purchases made on the Air Canada website were cancelled without notice*. All passengers involved weren't told by the airline, most only discovering they had no ticket when they arrived for their flights. [if interested, go to the article for more discussion]

Canadian Privacy Commissioner Raises Flag Over Planned U.S. Border Password Searches 🇨🇦

http://www.cbc.ca/news/canada/windsor/canadian-privacy-commissioner-raises-flag-over-planned-u-s-border-password-searches-1.4138151

Canadian privacy could be imperilled by apparent U.S. plans to demand cellphone and social media passwords from foreign visitors, a federal watchdog says. In a letter to the House of Commons public safety committee, privacy commissioner Daniel Therrien warns the *recent pronouncements* from the Trump administration *could mean intrusive searches - even at preclearance facilities in Canada*. In February, U.S. Homeland Security Secretary John Kelly suggested at a hearing that American officials could ask people entering the U.S. about the Internet sites they visit as well as passwords to help assess their online activities. Kelly's proposal prompted an American coalition of human rights and civil liberties organizations and experts in security, technology and the law to express "deep concern." *The Wall Street*

Journal reported last month that visitors to the U.S. could be forced to provide cellphone contacts and social-media passwords.

Canadian protections could be 'hollow'

Currently, passengers flying to American cities through eight major Canadian airports can be precleared there by U.S. Customs and Border Protection officers. The Commons public safety committee is studying legislation that would expand preclearance operations. Under the bill, U.S. searches at preclearance facilities would be governed by Canadian law, including the Charter of Rights and Freedoms. But Therrien says those protections appear to be hollow because they could not be enforced in court due to immunity provisions that significantly limit access to civil remedies for the actions of U.S. border officers carrying out preclearance duties.

In many situations, Therrien says in the letter, "it would appear that Canadians who wish to enter the U.S. will, at preclearance locations in Canada as well as at border points in the U.S., have to face the difficult choice of either accepting a search without grounds or forgoing their wish to travel to the U.S."

Under long-standing plans, preclearance is being expanded to Billy Bishop Toronto City Airport and Quebec City's Jean Lesage International Airport, as well as for rail service in Montreal and Vancouver. In March, Canada and the U.S. agreed to bring preclearance to other, unspecified locations. The Liberal government says the preclearance arrangements would strengthen security and prosperity while ensuring respect for the sovereignty of both countries.

Uncertainty at border since Trump elected

Efforts to move people and goods across the 49th parallel more quickly and efficiently have unfolded against a backdrop of uncertainty following Donald Trump's election in November. *The Nexus trusted-traveller cards of about 200 Canadian permanent residents were suddenly cancelled after Trump issued an executive immigration order banning visitors from several largely Muslim countries*. There have also been reports of minorities from Canada being turned away at the U.S. border.

8 Tips to Secure Those IoT Devices

http://www.networkworld.com/article/3085607/internet-of-things/8-tips-to-secure-those-iot-devices.html

[June20, 2016- good article, still best practices] As more and more Internet-connected devices find their way into our homes and businesses, it's important to remember that they represent a security risk. The Internet of Things (IoT) is growing rapidly, and *in the rush for convenience, our privacy and safety is often an afterthought. Leaving them unsecured is the digital equivalent of leaving the back door unlocked*. There are 5.5 million new things getting connected every day in 2016, as we head toward more than 20 billion by 2020, according to Gartner. That's an awful lot of devices. *They might bring all sorts of handy new features, but, whether it's the latest cutting-edge baby monitor or a wireless doorbell camera that links to your phone,* <u>it's also a network-connected computer and should be treated as such</u>.

Here are eight tips to help you secure those IoT devices.

1. Don't connect your devices unless you need to. *The first step is to consider what functionality you <u>need</u> from the device*. Just because your TV or fridge can connect to the internet, doesn't mean you definitely want to hook it up. Take a good look at the features it offers and <u>learn exactly what internet connectivity brings before you connect</u>.

2. Create a separate network. *Many Wi-Fi routers support guest networking so that visitors can connect to your network without gaining access to shared files or networked devices*. This kind of separation also works well for IoT devices that have questionable security.

3. Pick good passwords and a different password for every device. It's very important to pick strong passwords, but *you must also make sure that you pick a different password for every device*. *If a hacker manages to get one of your passwords, <u>they will typically try it with other services and devices</u>*. Reusing passwords is not a good idea [all security specialists emphasize this advice!]. Use a password manager to keep track of all your passwords.

4. Turn off Universal Plug and Play (UPnP). Sadly, UPnP can make routers, printers, cameras and other devices vulnerable to attack. It's designed to make it easier to network devices without configuration by helping them automatically discover each other. *The problem is that hackers can also potentially discover them from beyond your local network because of vulnerabilities in the UPnP protocol*. Is best to turn UPnP off completely. [what does this mean? Search online and ask a trusted source, like your Internet service provider support]

5. Make sure you have the latest firmware. If you want to make sure you have the latest security patches and reduce the chances of a successful attack, then you need to keep your firmware fully updated. *Vulnerabilities and exploits will be fixed as they emerge, so your IoT devices and your router need to be regularly updated*. Automate this wherever possible or set a schedule to check for updates every three months or so.

6. Be wary of cloud services. A lot of IoT devices rely on cloud services, but the requirement for an internet connection in order for something to function can be a real problem. Not only will it not work when the network is down, but it may also be syncing sensitive data or offering another potential route into your home. *Make sure you read up on the provider's privacy policy and look for reassurances about encryption and data protection*. [contact them and ask questions of you need help or clarification]

7. Keep personal devices out of the workplace. *Don't take your personal IoT devices to work*. There are *lots of potential security concerns for wearables*. Every enterprise should have a clear BYOD policy, and it's often a good idea to prohibit personal IoT devices from connecting to the network, or at least limit them to a guest network. [turn off Bluetooth and Wi-Fi when not actually needed, e.g. to listen to music on the device but you don't need to leave email and internet open – turn on airplane mode]

8. Track and assess devices. Businesses need to track everything connected to the network and monitor the flow of traffic. Devices need to be assessed to determine the level of access they should have, to keep them fully patched and up to date, and to protect data end-to-end to preserve its integrity. Unknown devices should flag an alert. *Understanding which devices are connected and what they're doing is a prerequisite for proper security*.

<u>If you're dealing with sensitive data or you're concerned about privacy, then make sure you have a long hard look at the IoT devices you're considering</u>. What security protocols do they support? How easy are they to patch? Do the providers have a proper privacy policy? *It's not safe to assume they're secure because all too often they simply aren't*.

Cisco: Secure IoT Networks, Not the Devices

http://www.networkworld.com/article/3198166/internet-of-things/cisco-secure-iot-networks-not-the-devices.html

With networking pros unable to trust the security of Internet of Things devices, Cisco says they should focus on implementing network-based security protections that limit the blast radius of IoT security breaches. This week Cisco unveiled a new package named IoT Threat Defense at the company's IoT World Forum in London. [this article is for information and does not endorse any vendor product, as noted in our disclaimer at the end of the Digest]

IoT Threat Defense combines seven separate offerings, including network-segmentation rule creator TrustSec, network behavior analytics platform Stealthwatch and device-visibility offering named Cisco Identity Service Engine. *Cisco's basic IoT security premise is that internet-connected devices cannot be trusted as secure. It says some device manufacturers are building security protections into devices, but that process is taking years to implement*. To protect IoT deployments, Cisco recommends that customers isolate the devices on network segments. Traditional segmentation using VLANS can become complicated at an IoT-deployment scale though, Cisco says.

Cisco's TrustSec platform that includes network segmentation capabilities. *"The logical move is to segment these devices to put them out of attackers' reach,"* Cisco says. *"If devices are compromised, organizations can prevent them from being used as pivot points to move through the network, and to activate incident response processes to protect the business."* IoT Threat Defense can detect anomalies in network traffic, block certain traffic and identify infected hosts. Cisco is targeting initial use cases in the medical, power utilities and automated manufacturing industries. While TrustSec and the other offerings that make up IoT Threat Defense are not new, Cisco's offering them as a bundled packaging specifically targeting IoT use cases. Cisco expects IoT Threat Defense to be available beginning in June; it did not release pricing information.

<u>IDC predicts the number of IoT endpoints will balloon from 14.9 billion at the end of 2016 to 50 billion by 2020 and up to 82 billion by 2025</u>. Despite the plethora of IoT devices already in the market, Cisco says enterprises still struggle with implementing IoT projects: A survey the company released at IoT World Forum says 60% of IoT projects stall at the proof-of-concept phase. Of projects that were completed, users deemed only one-quarter of them a success.

Judy Adware Infects Dozens of Google Play Apps

http://www.securityweek.com/judy-adware-infects-dozens-google-play-apps

Dozens of Android applications distributed via the Google Play store have exposed up to 36.5 million users to an auto-clicking adware, Check Point security researchers reveal. Dubbed **Judy**, the adware was initially discovered on 41 applications developed by a Korean company, some of which have been in the app marketplace for years. *All of these programs were updated recently and had between 4.5 million and 18.5 million downloads when the security researchers found the malware*.

<u>In a second campaign, the same piece of adware was found within applications from other developers as well, also with a large number of total downloads</u>, between 4 and 18 million (some apps had over 1 million downloads each). Potentially impacting over 36 million users to Judy, the two campaigns might have borrowed code from one another, the security researchers explain. *The malicious code managed to stay hidden in the Google Play store for a long time, as the oldest app in the second campaign was last updated in April 2016. All of the offending applications have been removed from the application storefront after Google was notified on the issue*. The crooks behind these campaigns managed to bypass Google Play's protection (known as Bouncer), by creating a seemingly benign bridgehead app that can establish connection to the victim's device. After the user downloads it from Google Play, the app silently registers receivers to establish a connection with the command and control (C&C) server.

Once the connection has been established, the server delivers the malicious payload, which includes JavaScript code, a user-agent string and URLs controlled by the malware author. *Even after infecting the device, the adware relies on communication with the C&C server to conduct its nefarious operations*.

"The malware opens the URLs using the user agent that imitates a PC browser in a hidden webpage and receives a redirection to another website. Once the targeted website is launched, the malware uses the JavaScript code to locate and click on banners from the Google ads infrastructure," Check Point explains.

The discovered malicious apps were developed by a Korean company named Kiniwini, which also develops apps for iOS and which is registered on Google Play as ENISTUDIO corp. Despite being created by a company, the offending apps engage into illicit activities by using victims' mobile devices to generate fraudulent clicks and revenue for operators. *Furthermore, Judy was also found to display a large amount of advertisements, some of which "leave users with no option but clicking on the ad itself*."

Despite users noticing the nefarious behavior, most of the applications have positive ratings, but it's not unusual for malicious apps to have high reputation, as cybercriminals can easily hide the app's real purpose or manipulate users into leaving positive ratings. Examples of such behavior would include DressCode or the recently observed fake System Update app.

Latest WannaCry Theory: Currency Manipulation

http://www.securityweek.com/latest-wannacry-theory-currency-manipulation

[May30] The recent WannaCry outbreak is still a mystery. We know what (ransomware), and how (a Windows vulnerability on unsupported or unpatched systems); but we don't know who or why. We're not short of theories: Lazarus, North Korea, some other nation-state actor, Chinese or Russian actors - *but none of these has gained general acceptance.*

The basic problem is that elements of Wannacry just don't make sense. The scale and rapidity of its spread, although not unprecedented, points to expertise and resources. This together with some code similarities has led to suggestions that it was a nation-state attack emanating from North Korea. But inefficiencies in collecting the ransom is not likely from a group as experienced as Lazarus; and the absence of any visible political motive throws doubt on the idea that any nation-state actor was involved.

Thycotic's cyber security and digital forensics expert, Joseph Carson, has an alternative theory: the motive behind Wannacry was effectively insider trading following currency manipulation. Bitcoin was the real target. <u>If he is right, it explains the efficiency of the attack (the primary motive) and the inefficiency of the ransom collection (which was neither part of nor important to the plan)</u>.

Talking to *SecurityWeek*, Carson explained that one common theory on the value of Bitcoin is an application of Metcalfe's Law. Metcalfe's law states that the value of a telecommunications network is proportional to the square of the number of connected users of the system (n2) (Wikipedia). Giovanni Santostasi, chief scientific officer at DeepWave and Fountain Health Technologies, has applied this to Bitcoin: "The exponential growth is driven by one factor only, not millions. The rate of adoption. Period. In fact there is a strong correlation (R2 = 0.82) between number of users and price."

<u>*This is Carson's starting point. If you want to manipulate Bitcoin value, he told SecurityWeek, you cause a sudden increase in the number of users*</u>. This is most easily measured by the number of Bitcoin wallets in existence. A global ransomware outbreak, demanding payment by Bitcoin, would certainly have such an effect: both direct victims and judicious organizations are likely to obtain wallets.

"WannaCry," he suggested, "was a sleight of hand, a deception. The ransomware was merely a mechanism to get a large number of people to open a Bitcoin wallet - and that by itself would drive up the

value of Bitcoin." It could almost be described as a version of insider trading based on a sophisticated form of 'pump and dump': the criminals could invest in Bitcoin, pump its value through encouraging the growth of wallets, and then dump the Bitcoin to take their profits.

This theory is supported by Bitcoin currency movement during May. The following details come from CryptoCompare.com. On May 1, Bitcoin was reported reaching an all-time high of $1,379.28. The price grew steadily and consistently until May 11 when it reached $1,817 on the eve of Wannacry. On May 12, WannaCry Day, it fell back by 3.93% to $1,776.95. Did criminals slowly drive up the price by their own investment in Bitcoin, ceasing further activity as soon as Wannacry was released?

On May 13, Bitcoin fell another 3.28% to $1,735.03; and again on May 14 by 2.99% to $1,684.44. *But it's what happened next that is interesting*. On May 17, CryptoCompare reported, "Bitcoin is up 5.82% at $1,785.22." On May 18 it was $1,821.24. On May 19 it was $1913. On May 20 it was $2,158, and it just kept going - until, on May 26, CryptoCompare reported, "Bitcoin has dropped 5.33% in the last 24 hours. *Volumes are quite high, with over $580M dollars exchanged in the USD market, more than half a billion. The Bitcoin pull back is associated with profit taking following several days of rally."*

During this period, Bitcoin peaked at $2720 - almost exactly twice the price it started the month. *The simple reality is that these figures would support Carson's theory: the primary purpose of WannaCry was a deceptive means of currency manipulation. This was currency manipulation on a massive scale*.

The Dirty Hackers Who Steal Passwords for Jealous Lovers

https://motherboard.vice.com/en_us/article/the-dirty-hackers-who-steal-passwords-for-jealous-lovers

For years, jealous lovers have bought malware to monitor their spouses' mobile phone or computer. But there's another often overlooked and related market that also brings surveillance much closer to home: *paranoid men and women who hire cheap hackers to grab their spouses' email or social media passwords*. Although the hackers and their techniques may not be very technically sophisticated, *these services can still present a threat, especially to those who may already be in an abusive relationship*.

"We will stand by your side when the most loved and believed *[sic]* one's in your life cheat on you," one site, called Hire An Hacker *[sic]*, reads. "Hire a hacker to clear all your doubts, and live peacefully."

These sort of sites aren't hard to find: a quick Google of certain phrases will likely return at least a few relevant results, and prices hover around $50 to a few hundred dollars. *But even sites that don't explicitly market to jealous lovers may provide the desired services anyway*.

Posing as a potential buyer on NeighborhoodHacker.com, Motherboard asked a customer support staffer whether the site offered hackers to find out if a wife was having an affair. "May I know what account or website would you like us to hack for you to find out?" the representative replied. *When Motherboard said the imaginary target would be a Hotmail or Facebook account, the employee said "In general, we can help you with that issue." Of course, there is no guarantee a customer of one of these so-called hackers will get what they pay for*. One scam report site flagged Hire An Hacker as a fraud, the owners of which allegedly demand more cash than advertised. *But the FBI and other law enforcement agencies have targeted and successfully prosecuted the administrators of several other very similar websites which were certainly hacking for clients*.

One of those sites was needapassword.com, *whose owners broke into nearly 6,000 email accounts*, according to a 2014 Department of Justice press release announcing related charges. "Is your spouse cheating with someone? Do you know who they are?" the now-defunct website read, according to the affidavit. "You have the right to read the personal thoughts your spouse is writing to others." Authorities also shut down five sites run from Romania, two in India, and one based in China, and the US charged three customers of hacker-to-hire sites too.

<u>Typically, these sort of sites are probably going to rely on phishing; that is, sending a phony login page or something similar to trick the user into entering their password</u>. *If you're worried* that someone, perhaps a husband, wife, or lover, may hire a hacker to obtain your password, *it could be worth locking your email and social media accounts with two-factor authentication. This means that someone logging into your account also needs a text sent to your phone, or a code generated by an app*. But, that may be complicated in some situations, especially *if your partner's abuse is physical as well as involving digital surveillance. In many cases, the best course of action will be to contact a professional for help*.

German Court Says Parents Have No Right to Dead Child’s Facebook Account

http://fortune.com/2017/05/31/facebook-parents-germany/

A German court rejected a mother's demand on Wednesday that Facebook grant her access to her deceased daughter's account. *In the ruling, which overturned a lower court's decision, the Berlin appeals court said the right to private telecommunications extended to electronic communication that was meant only for the eyes of certain people*. Privacy remains a sensitive issue in Germany due to extensive surveillance by Communist East Germany's Stasi secret police and by the Nazi era Gestapo. Memories of espionage were stirred anew by Edward Snowden's 2013 revelations of prying by the United States. In the Facebook case, the mother of a 15-year-old who was hit and killed by a subway train in Berlin in 2012 *had sought access to her daughter's account to search for clues as to whether the girl had committed suicide*. *Facebook had refused access to the account, which had been memorialized, meaning it was effectively locked and served as a message board for friends and family to share memories*. A regional court in Berlin had ruled in favor of the mother in late 2015, saying that the daughter's contract with Facebook passed to her parents according to German laws on inheritance. It had also said that the girl's right to privacy was not protected because she was a minor and it was up to her parents to protect her rights. *The appeals court said on Wednesday that the right to private telecommunications outweighed the right to inheritance, and that the parents' obligation to protect their daughter's rights expired with her death*.

Security Firm Asks EU to Investigate Microsoft

http://www.bbc.com/news/technology-40176599

Russian security software-maker Kaspersky has filed an anti-trust complaint against Microsoft with the European Commission. *It claims that the software giant is abusing its market dominance by pushing Windows 10 users towards its own anti-virus software*. The European Commission confirmed it had received the complaint. Microsoft said its security features "comply with competition laws". In a statement, it said it would "answer any questions regulators may have". "Microsoft's primary objective is to keep customers protected," it added.

In its statement, Kaspersky said: "These actions by Microsoft lead to a lower level of protection for users, a limitation on their right to choose, and financial losses both for users and security solution manufacturers." Kaspersky initially filed a complaint against Microsoft with Russia's Federal Anti-monopoly Service (Fas). *Since then, Microsoft has made some product changes, including to a status display window which suggested that users uninstall their existing anti-virus in favour of its own, dubbed Windows Defender*. Kaspersky has also filed a complaint to the German Federal Cartel Office.

Romania: Haven for Hackers Turned Cyber Sleuths

https://www.usatoday.com/story/news/world/2017/06/03/romania-hackers-turned-cyber-sleuths/102312234/

Razvan Cernaianu once surfed the Internet anonymously and easily broke into the computer systems for NASA, the Pentagon and Oracle. *Then he became part of a legion of hackers that turned Romania into a center of international cyber fraud investigators*. Now, the 25-year-old is co-founder of Cyber Smart Defense, a security firm with 12 employees, annual revenues of $1.45 million and offices in Belgium, Romania, the United Arab Emirates and Santa Barbara, Calif. *He's also one of a growing legion of former criminal hackers who have helped Romania - the second-poorest country in the European Union - punch above its weight in the tech industry*.

"As knowledge prevails in this area, companies will tend to hire people who have a past in (criminal) hacking," said Andrei Avadanei, chief executive of Bit Sentinel, an information security company based in Bucharest. “There are companies that appreciate a past in (that) area.” Romania's information and communication technology industry employs 120,000 engineers and generates around 6% of the country's gross domestic product, the fourth highest in the EU, according to the European Commission. Exports of tech services generated almost $3 billion last year, doubling over the past three years. The industry is set to generate $4.5 billion in two years, according to the Romanian Employers’ Association of the Software and Services Industry. Hackers transitioning to legitimate work is a long-awaited success story after the fall of communism in Romania in December 1989.

And Now, This:

Court Finds Man Guilty for Liking Defamatory Comments on Facebook

http://fortune.com/2017/05/30/defamation-comments-facebook/

In what appears to be a first, a court in Switzerland has fined a man the equivalent of over $4,000 just for clicking the "like" button on what a judge said were defamatory Facebook comments. The comments in question suggested that Erwin Kessler, who runs an animal-rights group, holds racist and anti-Semitic views. The defendant (who wasn't named in the court documents) clicked "like" on some of the comments and linked to some of the posts. Kessler has sued a number of people who participated in those discussions, which began in 2015 during a debate over which animal-rights groups should be allowed to participate in a vegan street festival, according to a Swiss newspaper.

Several of the people who made specific comments about Kessler have been found guilty of defamation, but Swiss legal experts said the defendant in the most recent case is the first to have been fined just for "liking" such comments. According to court documents, the judge in the case ruled that by clicking the "like" button, the defendant "clearly endorsed the unseemly content."

To complicate matters, Kessler was convicted of making racist comments (something that is illegal under Swiss law) in 1998, and briefly served time in prison. *But the judge in the recent case said that the defendant had failed to prove that the comments he "liked" were accurate*. Defamation law as it applies to social networks is a grey area in a lot of countries, including the United States, although the U.S. constitution provides a lot more protection for an individual's freedom of speech than some other jurisdictions. *A [U.S.] federal court found in 2013 that a "like" is protected speech under the First Amendment*.

…The Swiss case, however, appears to be the first in which a man has been found guilty of defamation just for clicking the "like" button on someone else's comments on Facebook. In her decision, the Swiss judge argued that by doing so, the man had made the comments "accessible to a large number of people," since Facebook showed them to all of his friends and followers. Doing this was an "affront to Kessler's honor," the judge ruled.

In a recent Canadian case, a woman was found guilty of making disparaging comments about her neighbor on Facebook. She was held responsible not only for the damage that her own comments caused, but also for subsequent comments made by her friends.

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.

****