

Security News Digest

December 12, 2017

(sent on December 13)

This Holiday Season is Here!
And so is the ['Online Shopping Safety' Quiz](#)

Give the Gift of Information Security Awareness!! – A Free Subscription to the Security News Digest. Just forward this email to your colleagues, family and friends, and they can learn how to stay safe online!

Anyone can subscribe: email OCIOSecurity@gov.bc.ca

We do not collect any information on our readers, and do not share our subscriber list with anyone.
(Make sure to add us to your Safe Senders list – don't be an "Undeliverable"!)

Uber Hack Prompts Formal Federal Privacy Investigation

<https://globalnews.ca/news/3909312/uber-hack-prompts-formal-federal-privacy-investigation/>

Privacy Commissioner Daniel Therrien has opened a formal investigation into the hack of Uber announced last month that **compromised the personal information of roughly 57 million customers around the world**. Uber CEO Dara Khosrowshaw announced in a blog post on Nov. 21 that **two hackers had stolen user data more than a year ago from drivers and customers that the company was storing on a third-party data storage application**. He did not disclose the number of customers or drivers in each country that were affected by the hack but later confirmed **the company paid the hackers \$100,000 to keep the breach secret**.

As Global News reported last month, news of the hack - and the fact that Uber had kept it secret for so long - quickly prompted calls for Canada to introduce tighter privacy regulations that would require companies to notify users when their private data is compromised. **Currently in Canada, companies are not required to notify users when their data is breached and companies rarely face fines or penalties for allowing customer information to be compromised.**

A spokesperson for Therrien had said last month the office had asked Uber to tell them how many Canadians were affected but that the company had indicated it could not do so. In an email to Global News, another spokesperson for the privacy commissioner indicated **they still cannot say how many Canadians had their private information accessed by the hackers**. “The privacy of riders and drivers is of paramount importance at Uber and we will continue to work with the Privacy Commissioner on this matter,” said Jean-Christophe de la Rue, spokesperson for the company in Canada.

Uber has said the data stolen included the names and drivers’ licences of 600,000 drivers in the United States along with “some personal information” of the users around the world. That information includes names, email addresses and mobile phone numbers but the company said it did not appear to include trip location history, credit card numbers, bank account numbers, social security numbers or dates of birth.

Bitcoin Fraud on the Rise as Canadians Swindled Out of \$1.7M This Year

<https://globalnews.ca/news/3908474/bitcoin-fraud-canadians/>

Canadians have been swindled out of more than \$1.7 million via scams involving cryptocurrencies such as bitcoin so far this year – more than double the amount during all of 2016. The Canadian Anti-Fraud Centre says that’s more than five times the amount people lost to these types of scams in 2015, which was roughly \$284,000.

As bitcoin becomes more popular with investors, sending the price above US\$17,000 mark last week, criminals appear to be increasingly turning to cryptocurrencies to extort payment from their victims as well. **These new figures come after police in Alberta, British Columbia and Ontario warned in recent months to beware of scams involving demands for a transfer of funds using bitcoin.** RCMP in Langley, B.C., last month said a woman received a call from what she believed was her husband’s

cellphone and someone posing as a police officer, asking for bail to secure her spouse's release. Police said the woman followed the caller's instructions and paid them \$5,000 in bitcoin, before receiving a call from her husband who was sitting at home and never arrested in the first place.

Yes, That Netflix Tweet is Creepy - and Raises Serious Privacy Questions

<http://www.zdnet.com/article/that-creepy-netflix-tweet-raises-serious-privacy-questions>

Netflix's ability to extrapolate detailed and specific viewing habits from its vast data set leaves troubling questions about its employees' access to personal customer information.

A snarky tweet posted by Netflix this weekend drew laughs - and concern. The tweet mocked a few dozen unnamed customers who've spent the past three weeks watching its heavily promoted "A Christmas Prince." The tweet, which at the time of writing had more than 103,000 retweets (and growing), became one of the streaming site's most popular tweets in just hours after it was posted. **The tweet, posted Sunday, said: "To the 53 people who've watched A Christmas Prince every day for the past 18 days: Who hurt you?" In saying so, Netflix not only admitted that the company can determine with accuracy how many of its over 100 million customers watch a certain show over a period of time, but also that some employees have access to that viewing data. No wonder some users found the tweet "creepy."**

It should come as no surprise that Netflix collects data on its users as it uses data analytics to algorithmically recommend new shows and to help improve its services. But some argued that Netflix was effectively abusing its privileged position to make jokes about its own customers. "My personal viewing habits are not fodder for tweets," said one Twitter user in response to the tweet.

We asked Netflix how many employees have access to customers' viewing habits and if there are any controls on who can access and what can be done with the data. A Netflix spokesperson would not address those specific questions, but sent ZDNet a canned statement.

"The privacy of our members' viewing is important to us," the spokesperson said. "This information represents overall viewing trends, not the personal viewing information of specific, identified individuals." In fairness, Netflix isn't the first company to use its vast wealth of data for marketing or advertising.

Spotify last year ran an advertising campaign that took some of the stranger, quirkier statistics from the company's year worth of streaming - like, "Dear 3,749 people who streamed 'It's the End of the World as We Know It' the day of the Brexit vote, hang in there." We also asked Spotify the same questions, but the company did not respond.

Using anonymized customer data in bulk for advertising isn't unlawful, so long as the information isn't publicly attached to a specific customer's name. Similarly, **under a little-known 1988 law, the Video Privacy Protections Act, Netflix and other streaming companies are barred from disclosing a consumer's viewing habits without consent.** But even when data is supposedly anonymized, it can be flawed.

Some years ago, Netflix released a data set of 100 million movie ratings by a little under half-a-million of its customers. The data was anonymized - each name was replaced with a unique identifying number - but researchers were able to unmask some users. Netflix eventually settled a class action suit brought under the 1988 privacy law for \$9 million, but the company did not admit any wrongdoing.

Netflix's ability to extrapolate detailed and specific viewing habits from its vast data set leaves troubling questions about employee access to personal customer information. **It's not only a reminder that companies collect and store but also generate vast amounts of data on its customers, and that companies can do almost anything they want with it** - even sending out snarky, creepy tweets to their 4.2 million followers.

Searchable Database of 1.4 Billion Stolen Credentials Found on Dark Web

<https://www.itworldcanada.com/article/searchable-database-of-1-4-billion-stolen-credentials-found-on-dark-web/399810>

A security vendor has discovered a huge list of easily searchable stolen credentials in cleartext on the dark web which it fears could lead to a new wave of cyber attacks. Julio Casal, co-founder of identity threat intelligence provider 4iQ, which has offices in California and Spain, said in a Dec. 8 blog his firm found the database of 1.4 billion username and password pairs while scanning the dark web for stolen, leaked or lost data. He said the company has verified at least a group of credentials are legitimate.

What is alarming in the file is what he calls "an aggregated, interactive database that allows for fast (one second response) searches and new breach imports." For example, searching for

“admin,” “administrator” and “root” returned 226,631 passwords of admin users in a few seconds. As a result, the database can help attackers automate account hijacking or account takeover.

Casal says the file is almost two times larger than the previous largest credential exposure, the Exploit.in combo list that exposed 797 million records. It is not entirely new data, but an aggregation of 252 previous breaches, including known credential lists such as Anti Public and Exploit.in, decrypted passwords of known breaches like LinkedIn as well as smaller breaches like Bitcoin and Pastebin sites. However, it does include information from 133 new breaches. “We’ve found that although the majority of these breaches are known within the Breach and Hacker community, 14 per cent of exposed username/passwords pairs had not previously been decrypted by the community and are now available in clear text,” said Casal.

Among other things, the database shows how some people still re-use passwords on many sites. For example, one person may have thought they were being safe by using an uncommon 10 digit password - but used it on six email addresses. **4iQ also used the database to generate a list of top common passwords. They include the usual suspects.** [article has a table showing the top 40 most commonly used, and worst, passwords – the top five are: 123456, 123456789, qwerty, password, and 111111 – these same ones come up on “worst password lists” published every year by security researchers]

There is no indication who created the database and tools, but whoever it was included Bitcoin and Dogecoin wallets for any user who wants to make a donation. In a column this morning SecurityWeek contributor Kevin Townsend quotes several experts worrying about how the database could be used. One said an attacker could just pick a target company and search for references to it in the list to find staff, contractors or suppliers. “This could give both an initial foothold into the company, or - if someone is already in - to help move around if credentials have been reused internally.”

MoneyTaker Hacker Group Steals Millions from US and Russian Banks

<https://www.bleepingcomputer.com/news/security/moneytaker-hacker-group-steals-millions-from-us-and-russian-banks/>

A cyber-criminal group believed to be operating out of Russian-speaking territories has hit at least 20 banks and financial companies and stolen millions of US dollars in the process. Details of these attacks were first made public in a report published yesterday [Dec 11] by Russian cyber-security firm Group-IB. The company believes this is a new group, different from other advanced criminal organizations that have hit the financial sector in the past, like the Carbanak, Cobalt, and Lazarus Group operations.

Researchers named this new group MoneyTaker, based on the name attackers gave to one of their hacking utilities.

MoneyTaker group began operations in 2016. According to Group-IB, MoneyTaker has started operations sometimes in 2016, hitting its first target - a Florida bank - in May 2016. Since then, the group has hit 14 US banks, a US services provider, a UK company, 3 Russian banks, and one Russian law firm. The attacks that hit banks have focused on infiltrating inter-banking money transfer and card processing systems such as the First Data STAR Network and the Russian Central Bank’s AWS CBR system. Attackers infiltrated one computer, then spread laterally, gathering any files and credentials they could, hoping to compromise a PC with access to the STAR or CBR networks.

Attackers studied bank networks by stealing documentation files. Evidence collected by Group-IB suggests attackers intentionally searched and stole internal documentation files to learn about bank operations in preparation for future attacks. In some cases, attackers also stole documents on SWIFT, another inter-banking money transfer system, and files on OceanSystems’ FedLink, a card processing system widely deployed across Latin America. Now, experts believe Latin America banks and banks utilizing the SWIFT system are in MoneyTaker’s crosshairs. The SWIFT team issued a report last month with recommendations on how banks could improve their security.

Attackers used fileless malware, legitimate apps. As for the “hacking” part of the MoneyTaker attacks, **Group-IB said the hackers’ activity was very hard to investigate.** Attackers used common and legitimate apps to carry out malicious operations and used a wide arsenal of malware families. **Each hack was different, showing that the group studied each target in fine detail and deployed only tools appropriate for those targets.** The hackers never focused on one bank system alone, and stole money from card processing systems, from ATM networks, and even installed POS (Point-of-Sale) trojans

when the hacked organizations weren't financial institutions and had no connection to a large inter-banking network.

According to Group-IB, the group used the MoneyTaker malware framework to hijack inter-banking and card processing operations, the ScanPOS malware for POS systems, custom screenshots and keylogging tools and the Citadel and Kronos banking trojans to move laterally inside networks. The table [in this article] shows tools used by MoneyTaker during their attacks.

In addition, MoneyTaker also used SSL certificates generated in the name of big brands to sign their malware, used one-time Yandex and Mail.ru email accounts, and employed the overdraft technique for cashing stolen funds with the help of money mules. Further, **the hackers also took the time to delete their entry points**, as Group-IB was not able to find the initial infection vector, and used a unique command-and-control server infrastructure that did not deploy any malware unless the download request came from a targeted bank's IP address range. Group-IB investigators said they forwarded all the data they gathered on this group to Europol and Interpol, as they suspect this will not be the last time we hear about MoneyTaker's operations.

Hackers Behind Mirai Botnet & DYN DDoS Attacks Plead Guilty

<https://www.hackread.com/mirai-botnet-hackers-2016-ddos-attacks-plead-guilty/>

A group of three hackers has pleaded guilty to their role in developing, spreading and using Mirai malware botnet to conduct large-scale Distributed Denial of Service (*DDoS*) attacks on some of Internet's most popular websites and Dyn DNS, a prominent Domain Name Servers (DNS) service provider.

In a proceeding that took place in US District Court for Alaska on November 28th, Paras Jha pleaded guilty to six charges including developing and operating Mirai botnet while Dalton Norman and Josiah White, his partners in crime also pleaded guilty to their role in the campaign in which Mirai was used for criminal activities. In January this year, Jha's father Anand Jha denied his son's role in Mirai's scheme and said "I know what he is capable of. Nothing of the sort of what has been described here has happened." However, according to the court documents released on Tuesday, Jha admitted his crime. Furthermore, court documents revealed that Jha erased the device he used to run Mirai on. Paras Jha "securely erased the virtual machine used to run Mirai on his device. Jha posted the Mirai code online in order to create plausible deniability if law enforcement found the code on computers controlled by Jha or his co-conspirators," said one of the court documents.

Damage caused by Mirai. On October 21st, 2016, **Mirai malware caused havoc by hijacking millions of IoT [Internet of Things] devices including security cameras and hit some of the most popular websites on the Internet including the servers of Dyn. The sites that were forced to go offline included Reddit, Amazon, New York Times, Twitter and hundreds of others.**

As a result, Internet services in the United States, India, Japan and some parts of Europe suffered major interruption. Like other botnets, Mirai also compromised Internet of Things (IoT) devices including security cameras and DVRs to carry attacks against DYN, Brian Krebs' blog and OVH hosting servers in France. Hackers also conducted click fraud through Mirai and made nearly 100 bitcoin that is more than \$1.6 million today due to a massive increase in Bitcoin's value. But the trio did not stop there, soon after targeting DYN, the source code for Mirai was leaked online that was later used by several other hackers to carry DDoS attacks.

The person who claimed to leak the source code stated his name as Anna-Senpai, however, on October 4th, 2016, security journalist Brian Krebs claimed Senpai is actually Jha, but Jha denied the allegation and his role in the development of Mirai botnet. According to Department of Justice's press release, Paras Jha has also admitted his responsibility for multiple hacks of the Rutgers University computer system.

"Paras Jha has admitted his responsibility for multiple hacks of the Rutgers University computer system," said Acting U.S. Attorney Fitzpatrick. "These computer attacks shut down the server used for all communications among faculty, staff, and students, including assignment of coursework to students, and students' submission of their work to professors to be graded. The defendant's actions effectively paralyzed the system for days at a time and maliciously disrupted the educational process for tens of thousands of Rutgers' students. Today, the defendant has admitted his role in this criminal offense and will face the legal consequences for it."

Plea agreements. According to [document] shared by Brian Krebs, under Jha's click fraud guilty plea agreement, he would hand over 13 bitcoin to the United States government. White, on the other hand,

has agreed to pay 33 bitcoin. The current price of 33 Bitcoin is more than \$547,469 while 13 Bitcoin is \$215,669.

This Fidget Spinner App is Sending Other Apps Data to Chinese Server

<https://www.hackread.com/this-fidget-spinner-app-is-sending-user-data-to-chinese-server/>

A few months ago, Bluetooth-enabled fidget spinners were in the news for blowing up and putting lives in danger. This time, these toys are in discussion for posing a threat to users' privacy and stealing their data. **According to Arun Magesh, an IT security researcher at Payatu Technologies, India; the AiTURE fidget hand spinner app on Play Store is collecting data of other installed apps and sending it to a server in China without their consent or knowledge.** Developed by Chinese firm Shenzhen Heaton Technology Co. Ltd, AiTURE supports Bluetooth connectivity to user's smartphone. Once the app is installed and connected to the phone, users can create their own patterns, single liners, and spin away.

Arun, on the other hand, conducted an experiment on several applications to check how do they transmit the data to the Cloud. After spending some time on AiTURE fidget hand spinner, he reverse-engineered the Bluetooth communications between the app and the fidget spinner. **Upon intercepting the app and the Internet connection, he discovered a huge chunk of data, that is being transmitted to a Chinese server.** The identified server's login page (api.e-toys.cn/passport/login) asks for username and password to access "Background System EToys" login system.

On further analyzing the data packets, the researcher noted that the app sends all the information about the apps installed on his phone to the server in a clear text. Arun believes this data could be used to target ads or even send remote exploits based on 0-days on other installed on phones. Although the app has only 1,000 – 5,000 installs, it still poses a significant threat to its users since it sends all the information on installed apps along with their version and installation time. **"If they are so smart. Why send it in plain text using HTTP and not HTTPS?? This makes me wonder if all cheap Chinese products which are sold at low prices are sold at the cost of our private data? Are we not safe from anything anymore," Arun told exclusively to HackRead.**

However, encrypted or decrypted, the question is why a fidget spinner app is sending user data to a server in China? Arun's curiosity about cheap Chinese products makes sense since this is not the first time a Chinese company has been caught getting their hands on user data. Previously, a Chinese mechanical keyboard manufacturer MantisTek was found spying on users through built-in keylogger in its GK2 model and sending the data to a server apparently hosted on Alibaba Cloud server. In September this year, researchers found popular Chinese keyboard app GoKeyboard collecting data and spying on millions of users. **Those Android users who are concerned about their privacy are advised to avoid downloading unnecessary apps from Play Store and third-party stores.** Remember, Play Store itself is home to tons of malware and malicious apps.

Car Rental Companies Failing to Protect Customer Data, Claims Privacy International

<https://www.v3.co.uk/v3-uk/news/3022575/rental-companies-failing-to-protect-customer-data-says-report>

Car rental companies and car-sharing schemes are failing to protect sensitive customer data, according to a recently published report by Privacy International. **The UK-based charity has found that car makers, and rental firms in particular, are negligent when it comes to protecting the privacy of drivers using the connected devices increasingly built-in to modern vehicles.** Companies are failing to look after a range of personal information, including locations they've visited, smart phone contents and places of residence.

As part of a research project, Privacy International rented a number of internet-connected cars in a bid to explore how information is collected and restored on their infotainment systems. **Every vehicle the charity rented exhibited serious privacy flaws when it came to personal data. The cars contained information about previous and current drivers, including locations visited and smartphone contacts.** The charity also got in touch with a number of car-schemes in Europe, the UK and the US to explore their internal security practices. However, none of them had what PI regarded as sufficient policies in place to ensure that personal information is protected.

And, out of the companies that participated in PI's research, all referred the charity to their terms and conditions. **They also said it's the responsibility of drivers to delete their data upon returning the car.** While many vehicles come with the option to "factory reset" the car, according to PI it's unclear how and what information is actually deleted. And only one car rental company is looking to adopt an internal

policy about deleting driver information, implementing it before the General Data Protection Regulation comes into force in May next year.

Millie Graham Wood, a solicitor at Privacy International, slammed the lack of any discernible policies at car rental firms to protect customer data. "This report shows how basic information, which could identify who we are and where we go, is currently left open and accessible to everyone on cars used by popular rental companies," she said. "We are calling on rental companies to make it simple and clear for people to delete their personal information when they return a rental car. We encourage individuals who see someone's data on the car to report it to the company." She added: "When we hire a car, the last thing on our mind is the data we are potentially giving away to companies, manufacturers, and the next driver. **"However, internet-connected cars know our current location, patterns of movement, connect to our smart phones to download our contacts and messages, may collect our browsing habits and know our music taste.** "The volume of data collected by infotainment systems and telematics units is growing."

Google Releases Tool to Help iPhone Hackers

https://motherboard.vice.com/en_us/article/d3x3dw/google-releases-iphone-ios-jailbreak-tool

Google has released a powerful tool that can help security researchers hack and find bugs in iOS 11.1.2, a very recent version of the iPhone operating system. The exploit is the work of Ian Beer, one of the most prolific iOS bug hunters, and a member of Google Project Zero, which works to find bugs in all types of software, including that not made by Google. Beer released the tool Monday, which he says should work for "all devices." The proof of concept works only for those devices he tested - iPhone 7, 6s and iPod touch 6G - "but adding more support should be easy," he wrote.

Last week, Beer caused a stir among the community of hackers who hack on the iPhone - also traditionally known as jailbreakers - by announcing that he was about to publish an exploit for iOS 11.1.2. Researchers reacted with excitement as they realized the tool would make jailbreaking and security research much easier.

While it might seem surprising that Google would release a tool to hack a device from a competitor, it actually makes a lot of sense. **The iPhone is one of the hardest consumer devices to hack, and researchers who can do that and are able to find bugs in it rarely report the bugs or publish the tools they use because they are so valuable.** But Google Project Zero researchers don't need the money, and their mission is precisely to make all software, especially that owned by other companies, safer. Google told Motherboard that Beer's goal is to allow other security researchers to explore and test the security layers of iOS without needing to develop and find their own exploits. In other words, Google gave other researchers a starting point, a base, to bootstrap their own research. The final goal, Google said, is to help security researchers find even more bugs and hopefully report them to Apple so that they get fixed. **Apple did not immediately respond to a request for comment, but the exploit has been patched. If you're not interested in jailbreaking your phone, you should update immediately.**

Luca Todesco, one of the most well-known iOS hackers in the world, told me that Beer's tool can definitely help researchers who don't have their own iOS bugs. Other iOS researchers such as Marco Grassi or Ryan Stortz have already speculated that Beer's exploit could be turned into a full jailbreak.

Over 26 Percent of Ransomware Attacks in 2017 Hit Business Users

<https://www.esecurityplanet.com/threats/over-26-percent-of-ransomware-attacks-in-2017-hit-business-users.html>

The proportion of ransomware attacks hitting business users rose from 22.6 percent in 2016 to 26.2 percent in 2017, according to a recent Kaspersky Lab report. "Welcome to ransomware in 2017 - the year global enterprises and industrial systems were added to the ever-growing list of victims, and targeted attackers started taking a serious interest in the threat," the report states. "It was also a year of consistently high attack numbers, but limited innovation." The number of new ransomware families dropped almost by half, from 62 in 2016 to 38 in 2017. At the same time, the number of modifications almost doubled, from 54,000 in 2016 to more than 96,000 in 2017.

Sixty-five percent of businesses hit by ransomware in 2017 lost access to a significant amount or all of their data, while 36 percent paid the ransom, 17 percent of them never recovered their data.

Three massive ransomware outbreaks - WannaCry in May, NotPetya in June and Bad Rabbit in October - greatly increased awareness of the threat. **"The headline attacks of 2017 are an extreme example of the growing criminal interest in corporate targets,"** Kaspersky Lab senior malware analyst Fedor Sintsyn said in a statement. "We spotted this trend in 2016, it has accelerated throughout 2017 and

shows no signs of slowing down." "**Business victims are remarkably vulnerable, can be charged a higher ransom that individuals and are often willing to pay up in order to keep the business operating,**" Sinitsyn added. "New business-focused infection vectors, such as through remote desktop systems, are not surprisingly also on the rise."

According to a separate Malwarebytes report, the number of ransomware attacks in the first three quarters of 2017 exceeded the total number in 2016 by 62 percent. Ransomware detections surged from less than 16,000 in September 2015 to hundreds of thousands in September 2017, an increase of almost 2,000 percent in two years. In 2017 alone, ransomware detections increased by more than 300 percent from 90,351 in January 2017 to 333,871 in October. The report suggests that ransomware has largely replaced the use of botnets, which decreased by almost 50 percent in the first three quarters of 2017.

"Knowledge of cybercrime and security best practices has to go across the organization, driven from the top down," the report states. "**With an endless array of potential vulnerability points, from reception to external vendors, an exchange of knowledge, awareness and insight is key to recognizing threats.**" "This idea of a CEO as a cyber security champion evokes an even bigger shift which can ultimately help businesses better protect themselves: **treating cyber security as an investment in trust, rather than a way to prevent losses or costs.**"

And Now, This:

Panic Button for Web Browsers Scrubs Away All Content Fast

<https://www.cnet.com/news/chrome-extension-safari-browser-nothing-on-the-internet-sideline-collective/>

Sick of the online clutter? Turn your Chrome or Safari browser into a blank slate with **the Nothing on the Internet extension**. There's now a panic button for web browsing, and it's the Nothing on the Internet extension for Chrome and Safari. Turn it on and it will wipe out all website content, leaving nothing but blank spaces behind.

Nothing on the Internet, brought to our attention by Lifehacker, delivers a fascinating look at the structural bones of a website. You might see a largely blank white canvas, or perhaps blocks of color reminiscent of a Mondrian painting. There's a sense of artful calm about it. No headlines. No ads. No walls of text. No bright images or auto-play videos. The extension comes from creative group Sideline Collective, which offers a compelling reason to use it: "**With the click of a button, witness all the noise and clutter that occupies so much of our 'busy' lives, that feeds our deepest fears and shallowest desires, witness it all vanish in an instant.**" That sounds pretty great.

Overall, the extension works well. You might see a header or a little text sneaking in on certain websites, but that's the exception. While Nothing on the Internet might seem frivolous at first blush, it could actually be an internet sanity saver. When you catch yourself getting lost in the online labyrinth, just hit that black box and engage the extension to remind yourself there's a world outside of your browser.

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 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.
