BRITISH COLUMBIA OCIO | Office of the Chief Information Officer

# Security News Digest
# March 14, 2017

## - March is Fraud Prevention Month -

**Take the Top Ten Scams Quiz on the**
**Better Business Bureau (BBB) Top Ten Scams for 2016**

**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

## Apache Vulnerability Exposes Canadian Government Websites to Hackers 🇨🇦

https://hotforsecurity.bitdefender.com/blog/apache-vulnerability-exposes-canadian-government-websites-to-hackers-17797.html

An easily exploitable zero-day vulnerability in Apache Struts 2 forced the Canadian government to take offline the websites associated with Canada Revenue Agency, used for filing tax returns, and Statistics Canada, just before the end of the fiscal year, according to Reuters. The online security breach was actually experienced by Statistics Canada, but the Canada Revenue Agency site also had to be shut down as precaution because it shared the same vulnerability. Officials assure citizens that the attackers were blocked quickly and got no sensitive data or tax-related information.

“We went after this one specifically because we recognized there was a specific and credible threat to certain government IT systems,” John Glowacki, a government security official, said at a press conference. Allegedly other countries “are actually having greater problems with this specific vulnerability,” he added without giving further details. *The new software bug appeared last week and was announced by the Apache Software Foundation that immediately released a patch*. Apache Struts, open-source software for Java apps, is used for websites by many organizations, including governments, banks, airlines and social networks. The vulnerability allowed hackers to access and take over web servers from a remote location.

## Canada Revenue Agency Online Services Running Again After Being Offline Since Friday 🇨🇦

http://www.cbc.ca/news/canada/cra-online-services-1.4021992

The Canada Revenue Agency is reporting that all of its online services are back in service after being down since Friday afternoon *due to an "internet vulnerability" that was discovered during website maintenance*. In an update posted on the CRA website, the agency said that as of 5 p.m. Sunday, individuals and businesses have been able to file electronically, make payments and access all other digital services*.* *"The CRA acted quickly to temporarily take down our online services, including electronic filing, and put in place the necessary maintenance security patches to ensure that all information and systems remained safe," the statement read*. "We took this action as a precaution, not as the result of a successful hack or breach."

The agency said tax returns that had already been filed were processed normally while the services were down and that Canadians should not "expect a delay in getting their refund." The CRA first took its website down as a precaution at midnight on March 10. It said it has worked around the clock over the past two days with other government departments to address the issue. Affected services included My Account, My Business Account, Represent a Client, the MyCRA mobile application, the MyBenefits mobile application, Netfile, EFILE and Auto-Fill My Return.

## 4 Charged in Massive Yahoo Hack, Including 1 Canadian 🇨🇦

http://www.cbc.ca/news/technology/russia-hackers-charged-yahoo-breach-1.4026006

The U.S. Justice Department says four people, including one who was taken into custody in Canada, have been charged in a mega data breach at Yahoo that affected at least a half billion user accounts.

The person arrested in Canada is Karim Baratov, named by Mary McCord, U.S. assistant attorney general. *Baratov, 22, is a dual Canadian-Kazakh national*. *Two of the defendants are Russian security officers and the other two are criminal hackers*. One of the defendants is on the list of the FBI's most wanted cyber criminals. The charges arise from a compromise of Yahoo user accounts that began at least as early as 2014. Though the Justice Department has previously charged Russian hackers with cybercrime - as well as hackers sponsored by the Chinese and Iranian governments - *this would be the first criminal case brought against Russian government officials*. It comes as federal authorities investigate Russian interference through hacking in the 2016 presidential election.
*Yahoo didn't disclose the 2014 breach until last September* when it began notifying at least 500 million users that their email addresses, birth dates, answers to security questions and other personal information may have been stolen. Three months later, Yahoo revealed it had uncovered a separate hack in 2013 affecting about one billion accounts, including some that were also hit in 2014.

## How Crooks are Getting Better at Imitating Texts, Emails from Banks 🇨🇦

http://www.cbc.ca/news/canada/nova-scotia/criminals-phishing-banks-fraud-scotiabank-infoalerts-scene-1.4017269
As criminals use emails and texts to phish for people's personal information in hopes of robbing bank accounts, *it's becoming increasingly difficult for the average customer to know what is legitimate communication from their bank and what is not*. "They [scammers] are much better at targeting their audiences now and doing a lot better job of making it look realistic and it becomes very confusing for people," said Sgt. Royce MacRae with the RCMP's Tech Crime Unit in Nova Scotia.
**Crooks mimic messages from bank** Brenda and Fernando Afonso learned the hard way how sophisticated these scammers are. The couple had been using Scotiabank's InfoAlerts service, which sends a text or email to an account holder every time their debit or credit card is used. It's a way to make sure all transactions are legitimate and keep track of any unauthorized use. *Then fraudsters sent messages that looked like they were from InfoAlerts to get into their bank account. "We were out one day and my husband got a text message saying his bank card had been used and he hadn't used it so he became concerned," Brenda Afonso told CBC News. "He logged in to check his account and when he did he was actually logging into a bogus account and they got all of his information." The fraudsters used the information they had obtained to clean out the $3,000 in the Afonsos' bank account.* The Afonsos thought bank insurance would cover their loss, but they were told Scotiabank would not be replacing the money because they had willingly given out their banking information.
**Phishing on the rise**
*Scotiabank has a highlighted message on the login page of its online banking website stating:*
"Scotiabank does not send text messages or emails that ask you for your password for online and mobile banking, Personal Identification Number (PIN) for either your ScotiaCard or credit cards, account numbers for any type of account, answers to your security questions, or access code for adding payees."
**Password request sent to SCENE members**
But the situation gets fuzzy for consumers in light of a recent email sent to Scotiabank customers. The bank is a partner of SCENE, a program where customers can earn points toward free movies and meals by using their Scotiabank cards. *SCENE sent out an email to its members on March 1, asking them to reset their password to access their account. The message included a link to reset the password. A CBC viewer who received the email was uncertain whether it was real, so she called the bank and was told it was a scam.* However, it turns out the email was real. ..Subsequently.. "SCENE proactively sent an email to its member base with a suggestion *to update passwords online* at scene.ca... to help our members keep their accounts safe."
**Whether to click or not click?**....As for those confused by emails and texts that seem to come from their bank, [or other companies where you have an account, the best] advice is not to respond to anything you receive online before first contacting your bank [or checking the website of the company].
[To Avoid Being Phished – Do Not Click on the Link in an email to reset your password, unless you requested a password reset via email. Copy and Paste the link into your browser and do the password reset on the website.]
Marketing professor Ed McHugh has a message for the banks. "Be clear. If you say you'll only send info through your website, don't send it via other means."
And Brenda Afonso has a message for consumers too. "Don't use a lot of those apps unless you really need to. Go back to basic banking as much as you can and know your account is not insured [when this happens]." *[If you respond to a phishing email by giving your account number and password, the banks*

*can and will say that you gave the information – you were not hacked, you were phished. This is valuable security awareness information!]*

## 'We are all doing it': Employees at Canada's 5 Big Banks Speak Out About Pressure to Dupe Customers 🇨🇦

http://www.cbc.ca/news/business/banks-upselling-go-public-1.4023575

Employees from all five of Canada's big banks have flooded Go Public with stories of how they feel pressured to upsell, trick and even lie to customers to meet unrealistic sales targets and keep their jobs. The deluge is fuelling multiple calls for a parliamentary inquiry, even as the banks claim they're acting in customers' best interests. In nearly 1,000 emails, employees from RBC, BMO, CIBC, TD and Scotiabank locations across Canada describe the pressures to hit targets that are monitored weekly, daily and in some cases hourly.

"Management is down your throat all the time," said a Scotiabank financial adviser. "They want you to hit your numbers and it doesn't matter how." CBC has agreed to protect their identities because the workers are concerned about current and future employment. An RBC teller from Thunder Bay, Ont., said even when customers don't need or want anything, "we need to upgrade their Visa card, increase their Visa limits or get them to open up a credit line." "It's not what's important to our clients anymore," she said. "The bank wants more and more money. And it's leading everyone into debt." A CIBC teller said, "I am expected to aggressively sell products, especially Visa. Hit those targets, who cares if it's hurting customers."

… The revelations about other banks came pouring in after Go Public revealed last week that front-line staff at TD were under pressure to sell customers products and services they may not need and that *some employees were breaking the law* to hit their sales revenue targets. ..Some of the big five bank employees said they're so stressed by expectations to hit sales targets, they're on medical leave. Others said they had to quit. ..While working in Waterloo, Ont., she says her manager also instructed staff to tell all new international students looking to open a chequing account that they had to open a "student package," which also included a savings account, credit card and overdraft. "That is unfair and not the law, but we were told to do it for all of them." (see article for more details)

## Trained Immigrants Needed for B.C.'s Tech Industry, CEO Says 🇨🇦

http://www.cbc.ca/news/canada/british-columbia/tech-industry-workers-1.4025094

**The B.C. Tech Summit** is in full swing at the Vancouver Convention Centre, and a lot of discussion this year has been around the demand for trained workers. This is the second year the provincial government has funded the summit, and Premier Clark has delivered a keynote speech both years. During this year's speech the Premier called on Ottawa to lower barriers for tech savvy immigrants trying to move to B.C. "While other countries are looking in, let's be a country and a province that is looking out ... that is building bridges to the world, that is welcoming people in, the best and the brightest from every corner around the globe," Clark said in her address to *5,000 delegates*.

Speaking with guest host Gloria Macarenko on *On The Coast*, *B.C. Tech Association CEO Bill Tam said a major challenge facing companies in B.C. is a lack of trained workers*. "It's been very tight," said Tam. "The number one issue for all the companies that we work with has been being able to attract the talent that they need to be able to grow their businesses." He said bringing trained workers from outside of the country and increasing the capacity of post-secondary institutions is essential for economic growth. ..Tam added Vancouver stands apart from other tech industries for its capability in virtual and augmented reality development.

## Google Inc Announces First Canadian 'Cloud Region' in Montreal, Allows Sensitive Data to Stay Within Borders 🇨🇦

http://business.financialpost.com/fp-tech-desk/google-inc-announces-first-canadian-cloud-region-in-montreal-allows-sensitive-data-to-stay-within-borders?__lsa=ebfa-96fa

Google is building its first cloud region in Canada, which it says will allow businesses to keep sensitive data within the country while also speeding up services like machine learning that helps better analyze information. Located in Montreal, the first Canadian Google Cloud Platform Region was announced during a keynote Thursday at the company's Google Cloud Next '17 conference in San Francisco. *The new region now lets customers such as large corporations move large amounts of information to online*

*storage without having to leave Canadian borders like in the past with Google Cloud*. ..Google said its main competitive advantage with Google Cloud's offerings is that as large enterprise customers want to move digital, it will not just store the information but also provide its algorithms to make more sense of the data.
…While Google Cloud services have already been available in Canada, having a local region means organizations that deal with sensitive data or are heavily regulated - such as financial institutions or the health care sector - are more comfortable and able to use online storage. However, the new region is expected to be a welcomed addition by many Canadian customers. "Canadians always love to know that their data is still on this soil, especially as there is legislation in the U.S. that allows the government to go into data centres under the Patriot Act," said Roland Gossage, chief executive of the Toronto-based e-commerce provider GroupBy Inc., in an interview. GroupBy's clients include banks, telecoms like Telus and retailers such as Urban Outfitters or Cabela's. "Some have applications that run on the other side of the border, but there is always the preference to have on-soil data centres."

## 'I felt like a fool': Convicted Fraudster Dupes Small Town with Reality Show Promises 🇨🇦

http://www.cbc.ca/news/canada/toronto/go-public-burger-wars-chris-robinson-dunnville-1.4013699

Residents of a small Ontario town are still reeling after learning a man claiming to be a TV producer - promising to put mom-and-pop restaurants on a reality show - is actually a convicted fraudster who is wanted in B.C. If restaurant owners Julia Marchese and Debb Davies could have written the script for the show they thought they were going to be in, the ending would have been a lot different. The pair thought they were getting the opportunity of a lifetime: the chance to showcase their restaurants on a reality show called *Burger Wars*, which sees restaurants compete for the best burger in town. Both women hoped the show would boost business for them and tourism for Dunnville, Ont., a town of fewer than 6,000 people south of Hamilton. ..So when a man from B.C. claimed to be a big-time TV producer and made big promises, the business owners jumped at the chance.
**Town pitches in** They say Christopher Robinson told them that once they were accepted as contestants on the show, all they had to do was give him $500, and gather thousands more in "sponsorship" money to get the show off the ground. Soon the entire town was pitching in, hoping to put Dunnville on the map. The local paper even wrote up a glowing story about what the show would mean for the restaurant owners and the community. On his Facebook page, Robinson claimed to have all the credentials and connections with all the right people. What the residents of Dunnville didn't know is Robinson pleaded guilty to one count of fraud under $5,000 in 2001. *Go Public also found that while Robinson was asking the people of Dunnville for money to produce a reality show, he was wanted in B.C. on three charges of fraud under $5,000. He failed to show up in court to answer to those charges last June, and a warrant was issued for his arrest. Months later, after an application process, Robinson contacted Marchese to say Julia's Bistro would be the first restaurant to be featured on his show Burger Wars Canada*.
**Summary of details on the fraud:** Marchese says Robinson told her he was trying to sell the show to Netflix, but the streaming service tells Go Public it hasn't heard of him or the show. *The company that owns the real Burger Wars also says it has never heard of Robinson*. Robinson has a history of naming businesses after already established companies. Marchese estimates town residents gave Robinson more than $2,000 in sponsorship funds for flights and advertising, in exchange for a promised mention in the show credits. They also donated time and money to help renovate her restaurant. Just days before the television crew was scheduled to arrive, Robinson cancelled, posting on Facebook that he had fired his director. He didn't reschedule the shoot and he didn't return the money residents had contributed to the project. The real host of the real *Burger Wars*, Cris Nannarone, says he was surprised when he heard Robinson, a stranger, was claiming he was the host of the show. "I was angry. I'm still angry," Nannarone says. He says his producers would never ask restaurant owners to pay for anything. The real *Burger Wars*, owned by Calgary-based Pyramid Productions, is no longer in production. Reruns are still being broadcast under licence to Canadian network Corus and U.S. network Scripps, which between the two, own Country Music Television Canada (CMT), the Cooking Channel and the Food Network.
*[**March is Fraud Prevention Month** – Fraud comes in so many forms. Protect yourself and others by doing all the necessary research and questioning whether something is "too good to be true" - Sadly, if it sounds "too good to be true", it probably isn't true.]*

## Oft-forgotten, Why the Humble Router Remains One of the Most Insecure Devices in Your Home

http://www.cbc.ca/news/technology/routers-cia-wikileaks-cyber-security-insecure-1.4017033

For all the time that we spend thinking about the security of our phones and laptops - about encryption, strong passwords and two-factor authentication - comparatively little attention is paid to the humble internet router. *The tiny box is probably one of the most important pieces of technology you have in your home. It's the one device through which all of your other devices connect to the internet*. But despite being responsible for such an important task, most routers remain hidden away, rarely monitored and even more rarely updated - if their software is updated at all.

It's why, *for intelligence agencies and criminals alike, routers - plentiful and often insecure - are ever-increasing targets for attack*. "Once you target a router, you don't just get access to one computer," says Eva Blum-Dumontet, research officer for London, U.K.-based Privacy International. "You get access to any computer" or device that connects to the internet through that router, too. Documents released by WikiLeaks this week that detail the breadth of CIA hacking tools underscore just how valuable that access is - and, according to privacy and security experts, how easy it is to get. "This is a very dramatic problem," said Blum-Dumontet. *While our phones and laptops have gotten more secure, she explained, "We're connecting to the internet through routers which are just literally, absolutely, atrocious in terms of security."*

Katie Moussouris, CEO and founder of U.S.-based Luta Security, called routers "one of the biggest, most lush attack surfaces that we have." Their software doesn't differ greatly from country to country. "And nobody really thinks about keeping those updated," Moussouris said, which leaves them especially vulnerable to attack. With access to a router, an attacker could passively spy on the contents of unencrypted traffic as it passes to or from the internet - or even between devices in the home. *A router could also be used to launch a cyberattack, as was the case last year when attackers hijacked thousands of home routers (among other devices) and used them to take large swaths of the internet offline. An attacker could even redirect users to fake websites - say, a website that looks like Facebook - designed to steal passwords or credit card information, or install malicious software*.

…Both Moussouris and Blum-Dumontet say there's "no incentive" for manufacturers to support their routers once they've been sold - not when they can sell a newer model the following year. It's part of the reason routers get so few security updates, and have so many security holes. (Further complicating matters, some routers pull double duty as cable or DSL modems too.) But the onus isn't so much on consumers to get smarter as it is device manufacturers to do better - and for consumers to demand they do so, experts say. That means more frequent updates, but also routers that are easier to update than most currently are, and designed from the start to be more secure. (see article for more)

[This is not to promote Shaw over other companies, but Shaw does provide customers with a combined router/modem, with the reason being that they can provide better tech support if their customers all use the same product, rather than each home having a different model of router.]

## Samas RansomWorm Snakes Through Whole Domains

https://www.infosecurity-magazine.com/news/samas-ransomworm-snakes-through/

A ransomware variant known as Samas RansomWorm is wreaking havoc on unsuspecting machines, gaining its name from its unusual propagation characteristics. *Whereas traditional ransomware only encrypts the machine the attacker is controlling, RansomWorm spreads inside throughout the entire network to encrypt every server and computer - and the backups. According to research from Javelin Networks, it executes what it calls the "Worm Triangle."*

"After gaining a foothold on a machine connected to the corporate domain, the attacker executes a three-part process: Steal domain credentials, identify targets via Active Directory (AD) reconnaissance, and move laterally," the firm explained, in a blog. "This process is the 'worm', and it spreads itself throughout the entire network." Generally, the attackers exploit front-facing servers for a known vulnerability, and once the machine is compromised, he or she steals domain admin credentials, making it possible to act as a legitimate user on the network. Because of the admin-level privileges, these domain credentials grant the attacker full access to any computer inside the domain, laying their files wide open for encryption via AD.

"Think of it as a master key that can unlock any computer," Javelin researchers said. *"Samas infects one computer, and then self-propagates through the network, infecting each and every endpoint and server until the whole corporation is locked down…With a few built-in commands, the attacker encrypted the* *entire environment from the inside, evading traditional defenses while leaving no evidence behind."* This has dramatic consequences depending on the industry. In a retail environment, a complete POS lockdown will impact sales. Or in a hospital, patient data goes dark. It's been a successful gambit: The group behind Samas was able to rack up $450,000 in just one year using this methodology, Javelin said, primarily targeting healthcare organizations.

## New Malware Variants Near Record-Highs: Symantec

http://www.securityweek.com/new-malware-variants-near-record-highs-symantec

The number of new malware variants that emerged in February 2017 was three times higher compared to January, nearly reaching the record-high levels registered in October 2016, Symantec reports. *Last month the security company registered 94.1 million malware variants, which marks a worrying increase* when compared to the 32.9 million seen in January and only 19.5 million in December. Furthermore, Symantec's Latest Intelligence for February 2017 reveals that *the Kovter malware family* is the driving force behind this uptick. The rate of email malware increased as well, reaching one in 635 emails in February, up from one in 722 the previous month. Despite that, the overall email malware rates remain low compared to previous months, most probably as the result of "a lull in activity from the Necurs botnet which has been quiet since late last year," Symantec says. The global spam rate registered a very small drop of only 0.1 percentage points in February, reaching 53.7% from the 53.8% registered in January. The Construction sector was hit the most, with a 59.28% spam rate, followed very closely by the Mining sector at 59.27%.

…Phishing attacks decreased last month as well, reaching one in 8,246 emails, down from one in 3,271 in January. The phishing rate declined across all industries, the researchers say. "While phishing rates declined last month, we also saw *a new tactic being used by smartphone thieves who are now attempting to phish their victim's login credentials in order to unlock stolen phones*. Stolen high-end smartphones can earn criminals a lot of money, but only if they can gain access to them. This latest trick shows the lengths thieves are willing to go to get into a device," Symantec reports.

## Beware! Pre-Installed Android Malware Found on 36 High-End Smartphones

http://thehackernews.com/2017/03/android-malware-apps.html

Bought a brand new Android Smartphone? Do not expect it to be a clean slate. *At least 36 high-end smartphone models belonging to popular manufacturing companies such as Samsung, LG, Xiaomi, Asus, Nexus, Oppo, and Lenovo, which are being <u>distributed by two unidentified companies</u> have been found pre-loaded with malware programs*. These malware infected devices were identified after a Check Point malware scan was performed on Android devices. *Two malware families were detected on the infected devices: Loki and SLocker*.

According to a blog post published Friday by Check Point researchers, *these malicious software apps were not part of the official ROM firmware supplied by the smartphone manufacturers <u>but were installed later somewhere along the supply chain</u>, before the handsets arrived at the two companies from the manufacturer's factory*. First seen in February 2016, Loki Trojan inject devices right inside core Android operating system processes to gain powerful root privileges. The trojan also includes spyware-like features, such as grabbing the list of current applications, browser history, contact list, call history, and location data. On the other hand, SLocker is a mobile ransomware that locks victims devices for ransom and communicates through Tor in order to hide the identity of its operators.

**List of Popular Smartphones Infected with Malware:** Galaxy Note 2, LG G4, Galaxy S7, Galaxy S4, Galaxy Note 4, Galaxy Note 5, Xiaomi Mi 4i, Galaxy A5, ZTE x500, Galaxy Note 3, Galaxy Note Edge, Galaxy Tab S2, Galaxy Tab 2, Oppo N3, Vivo X6 plus, Nexus 5, Nexus 5X, Asus Zenfone 2, LenovoS90, OppoR7 plus, Xiaomi Redmi, and Lenovo A850.

The malware backdoor offers its operator unrestricted access to these infected devices, from downloading, installing and activating Android malicious apps, deleting user data, uninstalling security software and disabling system apps, to dialing premium phone numbers. *This incident underscores the dangers of untrusted supply chains, and experts are quite worried about the security of the supply chain with reports of over 20 incidents where rogue retailers have managed to pre-install malware on new Android handsets*.

Here's How to Remove the Malware Infections: (see article) (Since the malware programs were installed to the device's ROM using system privileges, it's hard to get rid of the infections.)

**It's not the first time** when high-end smartphones have been shipped pre-installed with malicious apps that can covertly siphon sensitive user data. In December last year, certain low-cost Android smartphones and tablets were found to be shipped with malicious firmware that covertly gathered data about the infected devices, displays ads on top of running apps and downloads unwanted APKs on the victim's devices. In November, researchers discovered a hidden backdoor in the AdUps firmware of over 700 Million Android smartphones, which also covertly gathered data on phone owners and sent it to a Chinese server without the user's knowledge. Meanwhile, a flaw in the Ragentek firmware used by certain low-cost Android devices was also discovered that allowed attackers to remotely execute malicious code with root privileges, turning over full control of the devices to hackers.

## Dark Web Suffers After Anonymous Hacked Firm Hosting Child Porn Sites

https://www.hackread.com/dark-web-suffering-after-anonymous-hacking/

We previously informed you about the hacking of over 10,000 websites on the Dark Web by the notorious hacker group Anonymous. The group took down the servers of Freedom Hosting II (web hosting services that handled 11,000 or nearly 20% of all Dark Web websites) to teach child pornography distributors and addicts on the Dark Web a good lesson. Anonymous also leaked a majority of data from Freedom Hosting II, which included over 380,000 user records.

Now we have learned that after the abovementioned cyber-attack, the number of hidden services on the Dark Web has lowered significantly. This revelation was made after an analysis was carried out using OnionScan. It is an open source tool that helps in the investigation of content or websites present on the Dark Web. According to the OnionScan report, out of over 30,000 Tor-based hidden services, only 4,400 are active on the Dark Web currently. It is much lower in comparison to previous such scans, stated the OnionScan project operator Sarah Jamie Lewis. Lewis also stated that they believed Freedom Hosting II has not only removed "thousands of active sites," but its sudden dislike of hidden websites has encouraged other hosting service providers too. This is why, noted Lewis, the number of hidden services has reduced so much including the secure email platform Sigaint, which went offline unannounced in mid-February.

Here the question arises, why Tor-based services have been removed? The reason could be that a majority of users have started to perceive Dark Web as a platform dedicated to criminality oriented or illegal activities. Furthermore, it is a fact that just like maintaining anonymity on Tor is difficult, in the same manner hosting a hidden service on the Dark Web is daunting as it required high-level skills and technical abilities. As per the report of OnionScan, states Lewis: "The skills required to run a Tor hidden service make offloading that work to a 3rd party tempting, however as seen with Freedom Hosting, and the other leaks we have demonstrated, this relationship creates additional security risks - and may in the end completely compromise any anonymity or privacy."

### *And Now, This:*

## #OpBlueWhale: "Anonymous" Urges Teens to Quit Playing Suicide Game

https://www.hackread.com/anonymous-blue-whale-suicide-game/

[Note: a search on Google showed some older articles suggesting that the suicide stories are a hoax, but articles warning about teens being drawn into the Blue Whale challenge game have been published in numerous places, especially in the U.K. This article about Anonymous taking action appears in HackRead and is presented here to create awareness of the things going on that we should probably know about.]

A group of hacktivists connected to the online hacktivist group Anonymous is urging teens to quit taking part in a sinister game called Blue Whale. Since last year, this game has gained popularity in Russia and as a result, 130 teens have reportedly committed suicide.. (Editor's note: HackRead has so far been unable to independently confirm the exact number.) Blue Whale requires teens to accomplish weird tasks for 50 days straight such as harming themselves, sleeping and waking up at odd times, watching explicit and horror movies. Upon completing these tasks, these teens are told to kill themselves which unfortunately allegedly has caused deaths of possibly as many as hundreds of teens in Russia. Hurting oneself is the core part of this game. Just last week, two girls were found dead after falling from a 14-storey apartment. Serbian Times report that Yulia Konstantinova, 15, and Veronika Volkova, 16, were likely playing the Blue Whale' suicide game. While the investigations are still ongoing in Russia, the trend is still gaining momentum in the country with the help of social media platforms which are being used to

promote the game.  For example, Yulia Konstantinova posted a picture of a blue whale on her Instagram account before killing herself.
…Although reports cover the incident in Russia, the Anonymous hacker group is urging teens on the social media to stay away from such groups and people willingly or being forced to play this game.  In an exclusive conversation with one of the Anonymous hacktivists, HackRead was told that: “We launch that operation #OpBluewhale to save all children in Europe from that dangerous game.  Behind of that game is Russian, Romanian criminals.  We have found all moderators of that game, and we have all information about the moderators.  We will destroy that game.  We have already saved a lot of children from suicide.”
..Anonymous also shared exclusive screenshot in which they gave in-depth explaining how teens are being threatened to become the part of this game.   Currently, Anonymous claims they have identified some administrators involved in the game and also spoken with the kids and saved some lives.  The hacktivists vow to hunt down the culprits and mastermind of the whole while at the same time they are urging teens not to become part of such online games and report anyone bullying them online or forcing them to get involved in such sinister activities.

**Feel free to forward the Digest to others that might be interested.**
**Click Unsubscribe to stop receiving the Digest.**

For previous issues of Security News Digest, visit the current month archive page at:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest
To learn more about information security issues and best practices, visit us at:

**Information Security Awareness Team - Information Security Branch**
Office of the Chief Information Officer,
Ministry of Technology, Innovation and Citizens’ Services
4000 Seymour Place, Victoria, BC   V8X 4S8
http://gov.bc.ca/informationsecurity
OCIOSecurity@gov.bc.ca