BRITISH COLUMBIA OCIO | Office of the Chief Information Officer

Security News Digest
July 04, 2017

You are invited to visit our
Canada's Security Scene Quiz

Canada's Top Court Upholds Ruling that Ordered Google to Wipe References to Discredited Company 🇨🇦

http://globalnews.ca/news/3561856/google-datalink-court-ruling-canada/

The Supreme Court of Canada has upheld a ruling that ordered popular search engine Google to wipe out references to a discredited company. *The high court's 7-2 decision on Tuesday recognizes that Canadian courts have jurisdiction to make sweeping orders to block access to content on the Internet beyond Canada's borders. Justice Rosalie Abella said the only way to ensure that the injunction met its objective was to have the order apply where Google operates – all over the world*. "The problem in this case is occurring online and globally," she wrote on behalf of the high court's majority. "The Internet has no borders – its natural habitat is global."

Google was challenging a 2015 ruling by a British Columbia court that ordered it to stop indexing or referencing websites associated with a company called Datalink Technologies Gateways. The B.C. Supreme Court granted the injunction at the request of Equustek Solutions Inc., which was locked in battle with Datalink for allegedly stealing, copying and reselling industrial network interface hardware it created. Burnaby-based Equustek wanted to stop Datalink from selling the hardware through various websites and turned to Google for help. Initially, Google removed more than 300 web pages from search results on Google.ca, but more kept popping up, so Equustek sought – and won – the broader injunction that ordered Google to impose a worldwide ban. *Google fought back against the "worldwide order," arguing that Canadian courts don't have legal authority to impose such an injunction*. Its written argument to the Supreme Court called the injunction "an improper and unprecedented extension of Canadian jurisprudence."

Google's lawyers had argued that if the court upheld a broad international injunction, it might inspire less democratic governments to seek binding court orders in Canada that are more intrusive. The view was shared by New York-based Human Rights Watch, which was granted intervener status in the case. *The rights organization joined a coalition of civil liberties groups, as well as several news organizations, in arguing the Canadian courts were overextending themselves and threatening free speech across the globe*.

Equustek had the support of a coalition of Canadian publishers, authors, composers and filmmakers, along with an international federation of film producers. Barry Sookman, lawyer for several large music companies and other creative organizations who intervened in the case, praised the decision, saying it would "very likely have enormous implications around the world." The ruling will help holders of intellectual property rights but could also serve as a precedent in Internet-related cases involving privacy, defamation and cyberstalking, Sookman predicted. He said the ruling could provide a "general framework for analysing when an order can be made against a search engine to help stop the facilitation of whatever that wrong happens to be."

Government Spyware Targeted Mexican Opposition Party, Toronto Researchers Suggest 🇨🇦

http://www.cbc.ca/news/technology/mexico-government-spyware-opposition-nso-citizen-lab-1.4184494

Three senior opposition officials in Mexico, including a party leader, were targeted with spying software sold to governments to fight criminals and terrorists, according to a report by researchers at the University of Toronto. *The officials, who included conservative National Action Party (PAN) head Ricardo Anaya, received text messages linked to software known as Pegasus, which Israeli company NSO Group only sells to governments, the report by Citizen Lab said*. Mexican President Enrique Pena Nieto has asked

the attorney general's office to investigate charges that the government spied on private citizens, saying he wanted to get to the bottom of the accusations that he called "false."
Last week, Citizen Lab, a group of researchers at the University of Toronto's Munk School of Global Affairs, identified 12 activists, human rights lawyers and journalists who had also seen attempts to infect their phones with the powerful spyware. John Scott-Railton, one of a group of researchers at Citizen Lab who have spent five years tracking the use of such spyware by governments against civilians, said Mexico's case was notable for the number of targets and the intensity of efforts. "What we have already provided, in our prior reporting, is strong circumstantial evidence implicating the government of Mexico," he said.
Anaya, PAN Senator Roberto Gil Zuarth and Fernando Rodriguez, the PAN's communications secretary, received infectious messages in June 2016, when lawmakers were discussing anti-corruption legislation, the report said. "That the government spies, invading the privacy of people in this magnitude, is absolutely unacceptable," Anaya said in a statement. "We will not rest until those responsible have resigned, are prosecuted and imprisoned." Pena Nieto's office said in a statement that it "categorically refuses to allow any of its agencies to carry out surveillance or intervention of communications" except for fighting organized crime or national security threats, and only with court authorization. *Mexico's government purchased about $80 million worth of spyware from NSO Group, according to a report by the New York Times last week*.

Trump Travel Ban: What Canadian Residents Can Expect at the Border

http://globalnews.ca/news/3561826/trump-travel-ban-canadians-travelling-to-us/
The latest version of U.S. President Donald Trump's travel ban goes into effect Thursday [June29], meaning residents of six mostly Muslim countries will be barred from entering the United States. The U.S. Supreme Court has allowed a limited version of the ban - which includes visitors from Iraq, Iran, Libya, Somalia, Sudan and Yemen - for 90 days. The court will hear full arguments about the ban in October. While the ban has been heavily criticized as unlawful and discriminatory against visitors of Muslim faith, the Trump administration has argued that it is needed on security grounds. They have also placed a 120-day ban on refugees.
But how does all this affect Canadian residents? Ottawa-based immigration lawyer Bhramba Kullur says the ban's full implications will only be known after it's implemented - *but it's clear things will change*.
Should Canadian citizens and permanent residents be concerned?
Kullur says while the ban has been imposed on "so-called terrorist-producing countries," Canadian citizens and residents with origins in those countries could be impacted. That could mean extra questioning and searches, or even being denied entry to the U.S. The lawyer adds that often it's a matter of bias against certain names, in addition to country of origin. "If someone has a name that is Muhammad or Khan, they are scrutinized." How concerned Canadians should be is still unclear, Kullur said, explaining that much of the policy surrounding the ban hasn't been revealed. He adds that if the past is any indication, there will be issues faced by Canadian citizens as well as immigrants, such as the case of a Montreal-born woman who was told she needs a visa to enter the States.
How will permanent residents of Canada be treated at the border?
Immigration lawyer Negar Achtari says permanent residents of Canada will be treated according to the passport they show at the border. "Permanent residents are going to be treated differently than citizens," the Ottawa-based lawyer said. Like most nationalities, permanent residents will have to obtain a visa to enter the U.S., but that doesn't guarantee they'll be allowed into the country.
Reason for travelling makes a difference Achtari says those travelling for specific purposes, such as to see family, attend school, or a work conference will likely have an easier time entering the States. Those with connections to the banned countries who are travelling for leisure, or without family in the U.S, should have "lower expectation of being admitted," she said.
Should Canadians with origins from banned countries avoid the U.S.? Choosing to avoid the U.S. is a personal decision, Kullur says, adding that it depends on why people are making the trip. While knowing the risks, those with family or work in the U.S. may not have the choice. "There will be consequences. They may not be allowed in." *Achtari adds that the current ban is only 90 days, which means delaying non-urgent trips is an option*.
Will those travelling to the U.S. this week face delays, extra trouble? As with past implementations of Trump's travel ban, Kullur says *airports will struggle to deal with the many changes*. "When the Supreme Court upheld the ban, it came as a surprise to everyone, so in the implementation there will be

chaos." Travel in the upcoming days will be stressful, including for those working at border control, he said. "There will be a lot of frustration."

Advice for those travelling to the U.S *Achtari has two suggestions for those travelling to the United States: Be prepared. Have a back-up plan*. The lawyer says being prepared means having all the documents you will need, and knowing answers to the questions immigration officials may ask. For example, visitors should know their relatives' home address. "At the same time, know there's a possibility that admission may not be granted," Achtari said. "Have a plan B."

Saskatchewan Privacy Commissioner Expresses Mobile Security Concerns 🇨🇦

https://www.canadiansecuritymag.com/news/data-security/saskatchewan-privacy-commissioner-expresses-mobile-security-concerns

REGINA - Saskatchewan's privacy commissioner says it's time for "a culture of caution" for government organizations and the public as they navigate the digital world. *In his annual report, commissioner Ron Kruzeniski outlines nine areas of concern, including security breaches from inside workplaces, hacking from outside, as well as how government employees store emails and use smartphones*. Kruzeniski said one employee conduct that is worrisome is when a worker clicks on an attachment or a link in an email that could let in a hacker. "I have no doubt that we will have to spend a lot more time and energy collectively as a society protecting ourselves against this," he said Wednesday. "It appears that hackers have found an economic reason for doing so, whether it's ransomware or identity theft and/or selling data that they've mined by hacking into systems all over the world, it pays off."

Kruzeniski said he doesn't think the risk can be eliminated, but it must be reduced. *He said officials should have separate email accounts for personal and work use, and work data should be on a government server*. Saskatchewan Premier Brad Wall was criticized by the NDP Opposition last month for using a private email server to do government business. The NDP said it's risky and wrong for the premier to use a private server for government business. *Wall initially stood by the decision to use personal email accounts while working at home or on weekends. But a spokeswoman from the premier's office later said he would only use government email to remove any concern*. Kruzeniski also raised *concerns about privacy breaches on mobile devices*. He said employers need to be clear about what staff can do with their work-issued smartphones, particularly because those phones could have personal or health information about someone.

He questioned what could happen if an employee allowed their children to play with the phone at home. "The ideal world obviously is to carry two phones, but how many of you do and how awkward and cumbersome is it," he said. The commissioner said there is a risk of privacy breaches if there is a lack of strong policies and enforcement on smartphone use. *Richard Murray, deputy minister of Central Services, said people can use work phones for limited personal use, but children and spouses should not have access to them. He said if employees need access to critical or sensitive government systems, they must use a government-supplied device*. "Some ancillary use is permitted under the rules ... so if your child happens to give you a call, you've got a day-care issue or whatever, that's fine, we don't discourage that sort of thing," he said. "But we absolutely do discourage providing a government phone to the kids to play games on or something. That's what personal devices are for."

FICO Survey: More than One-Third of Canadian Firms Without Cybersecurity Insurance 🇨🇦

https://www.canadiansecuritymag.com/news/industry-news/fico-survey-more-than-one-third-of-canadian-firms-without-cybersecurity-insurance

[June1] "Canadian firms are ahead of the curve when it comes to cybersecurity risk insurance, but over one-third (36 per cent) have not taken out cybersecurity insurance at all." Those are key findings in a new survey conducted by research and consultancy firm Ovum for Silicon Valley analytics firm FICO, which *reveals that even among those that have insurance, only 18 per cent say they have cybersecurity insurance that covers all likely risks*. Although the survey showed the efforts Canadian organizations still have to take to ensure they are fully protected in the event of a cyber-attack, *it also shows that these organizations are "significantly more responsible" than many of their global counterparts when it comes to insurance - especially when compared to the U.S*. While only 16 per cent of Canadian organizations say they have no intention of taking out cyber-risk insurance, more than a quarter (27 per cent) of surveyed U.S. executives responded the same way. "Without cyber-risk insurance, organizations are leaving themselves in a very vulnerable position," said Kevin Deveau, vice-president and managing director of

FICO Canada. “It’s important for businesses to assess the strength of their cybersecurity defences and to make sure they are covered if they are faced with a data breach. The ripple effect of a breach can be felt throughout the organization for a very long time, *especially now that Canada’s Digital Privacy Act will require organizations to report any breaches to regulators and customers*.”

Microsoft Announces New Wave of Nagging Popups

https://www.bleepingcomputer.com/news/microsoft/microsoft-announces-new-wave-of-nagging-popups/

On Friday [June30], Microsoft announced details about two new types of nagging popups that Windows 10 users are going to be seeing starting this week. *Microsoft says it took the decision to show these alerts in an effort to improve the security of Windows 10 users, which the company feels would be more secure if they'd update to the latest version of Windows 10, nicknamed Creators Update, and released in April this year*.

First nagging popup aimed at users of Windows 10 v1507. The first of these nagging popups will only appear for Windows 10 users still running version 1507, the first version of Windows, released in June 2015. This version has reached End Of Life (EOL) on May 9, 2017, and Microsoft has stopped shipping monthly security updates as a result. In a support article updated last week, Microsoft says: If you're currently running Windows 10 version 1507, you’ll receive a notification that your device needs the latest security updates and will attempt to update your device.

Second nagging popup focused on new privacy settings. The second set of nagging popups is *aimed at all users who have yet to update to the Creators Update*. "If you have not already taken this update, starting this week, *we will prompt you to review your privacy settings*," Microsoft says. "You can choose to postpone this process up to five times with the next prompt asking for confirmation of your privacy settings."

With the Creators Update, Microsoft introduced new privacy settings to comply with EU regulation. Every user that updated to the Creators Update was forced to review the new privacy settings before being allowed to update. Via this new popup, Microsoft will be nagging users to review their privacy settings in advance of updating. *It is unclear if by reviewing the new privacy settings, users are unwittingly giving the go-ahead to update their computers to the Creators Update*. In a blog post, Microsoft said that users still have "choice over when that update happens," but did not mention anything about having the option to decline the Creators Update, or if this means they agree to the update.

It is also worth mentioning that Microsoft published the news about upcoming Windows 10 nagware on a late Friday afternoon, right at the start of the July 4 [and July 1st] weekend. In PR and marketing, this is called a "Friday bad news dump," a term meant to describe the practice of publishing bad news ahead of weekends or holidays in an attempt to avoid media and user scrutiny.

Ukraine Cyber-Attack: Software Firm MeDoc's Servers Seized

http://www.bbc.com/news/technology-40497026

Police in Ukraine have seized the servers of an accountancy software firm, which is believed to have unwittingly helped spread malware that attacked many global firms last month. Intellect Service has denied that its software helped spread the malware. *But security experts have said that some of the initial infections were indeed spread via a malicious update to MeDoc. It is Ukraine's most popular accounting software.*

The cyber-attack - a variant of an earlier virus called Petya - hit businesses around the world including the shipping firm Maersk and the marketing giant WPP. It was initially thought to be a ransomware attack designed to make money for the hackers behind it. But some security firms now think that it was deliberately designed to destroy data and targeted Ukraine. The head of the country's national Cyberpolice unit had previously alleged that Intellect Service had ignored repeated warnings that it needed to improve its security in advance of the attack. "They were told many times by various anti-virus firms," Col Serhiy Demydiuk told the Associated Press news agency. "For this neglect, the people in this case will face criminal responsibility."

In a separate interview with Reuters, the father and daughter team who run Intellect Service said they were not responsible. "What has been established in these days, when no one slept and only worked? We studied and analysed our product for signs of hacking - it is not infected with a virus and everything is fine, it is safe," said Olesya Linnik, managing partner at Intellect Service. "The update package, which was sent out long before the virus was spread, we checked it 100 times and everything is fine."

Security experts, including Microsoft, Cisco and Symantec, said that they all have evidence that the malware was spread via an update to the tax software program MeDoc. It is believed that around 80% of companies in Ukraine use the software, which allows clients to send and discuss financial documents internally as well as file them with the government's tax department. Ukraine police said that the family could face criminal charges if it is confirmed that they knew about the infection but took no action.

Cyber-Attack was About Data and Not Money, Say Experts

http://www.bbc.com/news/technology-40442578

The Petya malware variant that hit businesses around the world may not have been an attempt to make money, suspect security experts. The malicious program demanded a payment to unlock files it scrambled on infected machines. *However, a growing number of researchers now believe the program was launched just to destroy data. Experts point to "aggressive" features of the malware that make it impossible to retrieve key files*.

Cashing out Matt Suiche, from security firm Comae, *described the variant as a "wiper" rather than straight-forward ransomware. "The goal of a wiper is to destroy and damage," he wrote, adding that the ransomware aspect of the program was a lure to generate media interest*. Although the Petya variant that struck this week has superficial similarities to the original virus, it differs in that it deliberately overwrites important computer files rather than just encrypting them, he said. *Mr Suiche wrote: "2016 Petya modifies the disk in a way where it can actually revert its changes, whereas, 2017 Petya does permanent and irreversible damages to the disk."*

Anton Ivanov and Orkhan Mamedov from Russian security firm Kaspersky Lab agreed that the program was built to destroy rather than generate funds. "It appears it was designed as a wiper pretending to be ransomware," they said. *Their analysis of the malware revealed that it had no way to generate a usable key to decrypt data*. "This is the worst case news for the victims," they said. *"Even if they pay the ransom they will not get their data back."*

A veteran computer security researcher known as The Grugq said the "poor payment pipeline" associated with the variant lent more weight to the suspicion that it was more concerned with data destruction than cashing out. "The real Petya was a criminal enterprise for making money," he wrote. "This is definitely not designed to make money." The Bitcoin account associated with the malware has now received 45 payments from victims who have paid more than $10,000 (£7,785) into the digital wallet. The email account through which victims are supposed to report that they have paid has been closed by the German firm hosting it - closing off the only supposed avenue of communication with the malware's creators.

Organisations in more than 64 countries are now known to have fallen victim to the malicious program. [A Cadbury factory in Australia halted production while it dealt with problems caused by the Petya malware variant.] The latest to come forward is voice-recognition firm Nuance. In a statement it said "portions" of its internal network had been affected by the outbreak. It said it had taken measures to contain the threat and was working with security firms to rid itself of the infection. <u>The initial infection vector seems to be software widely used in Ukraine to handle tax payments and about 75% of all infections caused by this Petya variant have been seen in the country</u>. <u>A government spokesman for Ukraine blamed Russia for starting the attack</u>. "It's difficult to imagine anyone else would want to do this," Roman Boyarchuk, head of Ukraine's cyber-protection centre told technology magazine Wired.

Computer security researcher Lesley Carhart said the malware hit hard because of the way it travelled once it evaded digital defences. Ms Carhart said the malware abused remote Windows administration tools to spread quickly across internal company computer networks. "I'm honestly a little surprised we haven't seen worms taking advantage of these mechanisms so elegantly on a large scale until now," she wrote. Using these tools proved effective, she said, because few organisations police their use and, even if they did, acting quickly enough to thwart the malware would be difficult. <u>The success of the Petya variant would be likely to encourage others to copy it, she warned. "Things are going to get worse and the attack landscape is going to deteriorate," said Ms Carhart</u>.

How does the new ransomware spread?

*Typically ransomware spreads via email **[phishing!!]**, with the aim of fooling recipients into clicking on malware-laden files that cause a PC's data to become scrambled before making a blackmail demand*. *But other ransomware, including Wannacry, has also spread via "worms" - self-replicating programs that spread from computer to computer hunting for vulnerabilities they can exploit*. The current attack is thought to have worm-like properties.

Several experts believe that one way it breaches companies' cyber-defences is by hijacking an automatic software updating tool used to upgrade an tax accountancy program. Once it has breached an organisation, it uses a variety of means to spread internally to other computers on the same network.
One of these is via the so-called EternalBlue hack - an exploit thought to have been developed by US cyber-spies, which takes advantage of a weakness in a protocol used to let computers and other equipment talk to each other, known as the Server Message Block (SMB).
Another is to steal the credentials of IT staff and then make use of two administrative tools - PsExec, a program that allows software installations and other tasks to be carried out remotely, and WMIC (Windows Management Instrumentation Command-line) a program that lets PCs to be controlled by typing in commands rather than via a graphical-interface. Once a PC is infected, the malware targets a part of its operating system called the Master File Table (MFT).
It is essential for the system to know where to find files on the computer. The advantage of doing this rather than trying to encrypt everything on the PC is the task can be achieved much more quickly. Then, between 10 and 60 minutes later, the malware forces a computer to reboot, which then informs the user it is locked and requires a payment from them to get a decryption key.
[If you are hit with a ransomware message on your screen, remember to Disconnect from the Network, then follow the appropriate procedure for reporting.]

6 Ways Security Pros Unwittingly Compromise Enterprise Security

http://www.csoonline.com/article/3204598/security/6-ways-security-pros-unwittingly-compromise-enterprise-security.html

That executives bypass security controls due to a lack of engagement between security and business decision makers seems logical, but the C-suite folks are not the only ones guilty of self-defeating behavior that creates more risk. Security professionals also do things that unwittingly introduce risks and compromise enterprise security. Here's a look at six self-defeating behaviors you should avoid:

1. Downloading tools that introduce risk

There are some security decision makers who - even though they are trying to do the right thing - take liberties to make their days easier. Perhaps they are afraid of their executives who want bypasses to do their work. Maybe it's that they themselves want a certain tool. Either way, they download tools and introduce risk.

2. Defaulting to 'trusting their guts'

Bay Dynamics co-founder and CTO Ryan Stolte said *half of the security alerts coming in are issues that security professionals think they have seen before*. So, they default to what they know, do what they've done before, and move on to the next alert. They recategorized, and that’s sort of sweeping it under the rug, Stolte said. People aren't meaningfully saying I’ve been breached and I want to hide it, but they sweep a lot of stuff under the rug.

3. Cutting corners and misconfiguring technology because they’re focused on deployment

Even when security practitioners decide to leverage technology, they end up cutting corners when they focus on deployment but misconfigure the technology. Lucas Moody, vice president and CISO at Palo Alto Networks, said, "Security professionals focus on the outcomes that the technology promises. The tough part is behind the technology. The work is once the technology is in place, but they are not carrying it through in the configuration." *It's self-defeating to deploy technology that requires downstream security operations work without focusing on configuration*. Instead, security professionals react to something. A tool is deployed that will help them find malware, but they don’t put in the processes behind that to go and find the malware, Moody said.

4. Patching reactively

As is evidenced in the expansion and prevalence of ransomware, a lot of organizations are patching reactively. *"It's relatively easy to quickly roll out patches, but we are doing it after things are felt instead of putting in a process to proactively deploy patches,"* Moody said. *To be fair, patching isn't always easy for every organization. Security practitioners need to consider whether a patch will disrupt the workforce or complicate end user interaction*. Because security professionals don’t want to introduce the friction that comes with patching, they decide to put it off until next week or two months from now. That is not explicitly cutting corners as much as it is a fact of having 10 things they are focused on, Moody said.

5. Investing in detection vs. prevention

Where and how to invest can also be self-defeating decisions. Investment in detection vs. prevention has caused problems, said Moody. Whether it's that the tool wasn’t robust enough to do prevention work or that it was the old-school way of thinking, security professionals invested in detection, focusing on the alarms instead of the prevention.

6. Paying ransoms

Another bad investment decision is choosing to pay ransoms when hackers hit them with ransomware. If you back up your systems, you can avoid this. Paying ransoms is "a ridiculous way to deal and puts incentives in the wrong hands. Most large organizations have the means and the appetite to invest in backup systems," Moody said.

Germany Braces for Cyberattacks at G20 Next Week

https://www.cnet.com/news/germany-braces-for-cyber-attacks-at-g20-next-week/

Protests at next week's G20 summit in Hamburg, Germany, could also come from all over the internet. And that's what's worrying Germany's top cybersecurity officials. Dozens of experts will stand by at a 24/7 command center among the 20,000 police with dogs, horses and helicopters there to deal with potential physical violence from the expected tens of thousands of protesters, reports Reuters. "As the national cybersecurity agency ... we're concerned about everything from (persistent threats) to groups like Anonymous and LulzSec that could be planning political protests using cyberattacks," said Arne Schoenbohm, president of Germany's Federal office for Information Security, in an interview with the news agency. Besides political protests from hacker groups, Schoenbohm is also concerned about attacks from cells linked to foreign governments, including Russia, which have been targeting Germany's political parties and think tanks ahead of the country's national elections in September.

Hacker Steals Millions of Accounts from Internet Radio Service 8tracks

https://motherboard.vice.com/en_us/article/mbjm83/hacker-steals-millions-of-accounts-from-internet-radio-service-8tracks

The data includes usernames, email addresses, and hashed passwords. Millions of accounts for internet radio service 8tracks are being traded on the digital underground, judging by a set of stolen user details obtained by Motherboard. *8tracks is a cross between a social network and an internet radio site, allowing users to stream custom playlists. The site offers both free and paid accounts which only for ad-free listening*.

Motherboard obtained a dataset of around 6 million 8track usernames, email addresses, and hashed passwords. *For-profit breach notification site LeakBase provided Motherboard with the data, and claims that the full dataset comprises of around 18 million accounts*. The passwords appear to be hashed with the SHA1 algorithm, *meaning hackers may be able to crack the hashes and obtain some of the original passwords*. *Several users in the data confirmed they signed up to 8tracks, with some signups stretching back to 2008*. Motherboard also independently confirmed that a selection of email addresses included in the data did correspond to accounts on the site by trying to create new accounts with them. In every case, this was not possible because the email address was already linked to an 8tracks account. 8tracks told Motherboard it was preparing to inform customers of the breach, and that it had identified and plugged the attack vector used by the hacker.

<u>"We believe the vector for the attack was an employee's GitHub account, which was not secured using two-factor authentication," 8tracks wrote in a blog post</u>. "If you signed up via Google or Facebook authentication, then your password is not affected by this leak," the post added, and said that *the stolen data only included those who had signed up via email*. The stolen data did not include any credit card information or other payment data.

The lesson: *Some of the users Motherboard spoke to couldn't remember which password they had used to sign up to the service. This means they did not know which other sites used the same password*. Even for sites that you may only create a free account on, it is always worth generating a unique password with a password manager. <u>That way, even if that site you used years ago is hacked, an attacker isn't going to be able to use your old password on any other services that use it</u>.

Amazon and eBay Images Broken by Photobucket's 'Ransom Demand'

http://www.bbc.com/news/technology-40492668

Thousands of images promoting goods sold on Amazon and other shopping sites have been removed after a photo-sharing service changed its terms. EBay and Etsy have also been affected, in addition to many forums and blogs. *The problem has been caused by Photobucket introducing a charge for allowing images hosted on its platform to be embedded into third-party sites*. The company caught many of its members unaware with the change, prompting some to accuse it of holding them to ransom. Denver-based Photobucket is now seeking a $399 (£309) annual fee from those who wish to continue using it for "third-party hosting" and is facing a social media backlash as a consequence. The BBC received an automated response when it tried to contact the company and is still seeking comment. *Photobucket has been online since 2003 and says it has more than 100 million customers and more than 15 billion images on its servers. Part of its attraction with small retailers was the fact that its ad-supported "free" accounts could be used to upload images of goods to a single destination from where they could be pushed to multiple outlets*.

On 26 June, however, the company published a brief note advising users to "take a moment to review our updated terms and policies". About 500 words into the linked document was a declaration that free accounts would no longer permit image-linking to third-party sites. *Many users realised the change only when their embedded images were replaced by graphics saying their Photobucket accounts needed to be updated*. ..Some sellers unwilling to pay the fee have handled the change by uploading their product photos to a rival service. *But the new policy has also affected historical social media posts, blogs and forums that were reliant on Photobucket*. One of those affected is Stampboards, a forum with more than 17,000 members who discuss postage stamps and share images of them. Many of its pages are now filled with Photobucket's upgrade demands instead of the photos of stamps it once showed. "They are holding you to ransom," the site's administrator, Glen Stephens, told members, advising them not to pay the fee. "You have no guarantee they will be in business... in a month the way this disaster is rolling out." <u>But one expert said the public needed to be aware of the risks of relying on any free image service</u>. "There's a lot of websites out there looking for advertising, and there's a finite amount of advertising spending to go round," said Nigel Atherton, editor of Amateur Photographer magazine. "And any photo gallery and storage site like this that relies on ads to offer a free service can only continue to do so if they have enough money coming in. *"So, if you put all your photos into any site or app like this where it's not clear how they are going to continue financing their business, then it could come back and bite you at some point in the future."*

South Korea’s Largest Ethereum Exchange Was Hacked

https://motherboard.vice.com/en_us/article/bjxnjw/south-koreas-largest-ethereum-exchange-was-hacked

South Korea is a leader in the ethereum cryptocurrency; a full 20 percent of global ether trades are exchanged for <u>South Korea's currency, the won</u>. Now, all the attention appears to have attracted hackers. *Last week, customer information and allegedly "billions" of won were stolen from South Korea's largest exchange for buying and selling ether as well as it's more popular and established cousin <u>bitcoin</u>*. South Korea-based Bithumb is the fourth largest cryptocurrency exchange in the world by volume, and the second largest ethereum exchange behind China's OKCoin. English-language details are scarce right now, but the government-funded *Yonhap News* reported that Bithumb contacted South Korea's cybercrime watchdog on Friday after it learned of the hack. *According to Yonhap, a Bithumb employee's home computer was hacked and information on 30,000 customers was stolen, although no passwords were compromised, according to the exchange*. *Yonhap* also reports that South Korean officials are now investigating the hack.

Despite Bithumb's alleged claim that no passwords were stolen, South Korean users are reporting that funds were stolen from their accounts on the Bithumb exchange. On Naver, South Korea's version of Reddit, a subforum for the hack <u>features numerous posts from users claiming to have lost funds in the hack</u>. One thread title reads, "I was hit. 7,100,000 won," which equates to around $6,000 USD. Bithumb did not respond to Motherboard's request for comment in time for publication.

If customer funds were indeed stolen from Bithumb customers, <u>the hack is just another reason why experts argue that it may not be wise to entrust your funds to a third party company</u>. *In April of this year, a smaller South Korean cryptocurrency exchange was hacked and lost millions of dollars USD of customer funds*.

<u>Other options besides storing your funds with a third party for ethereum users</u> include storing the private keys that control their funds on hard drives that are not connected to the internet. This isn't as convenient (or maybe even beneficial, if you're a day trader), but gives hackers fewer openings. As ethereum and cryptocurrencies in general continue to rise in value and garner mainstream attention, we're sure to see more hackers come along for the ride.

Citizens Advice Warning Over 'Phantom Goods' Scams

http://www.bbc.com/news/business-40441361
A rising number of people are being caught out by "phantom goods" scams - when items are bought online but are never delivered, Citizens Advice says. Cars, flights, furniture and insurance are among the goods and services which buyers think they are getting at a bargain, but which do not exist. The charity said nearly all of those tricked failed to get their money back.
The average loss was £1,100, it said as it urged people to take their time over online purchases. "With so many people shopping online to compare deals, scammers are using numerous tactics to target people with phantom goods," said Gillian Guy, chief executive of Citizens Advice. "They are drawing people in with cut-price deals *and then persuading people to buy items with phoney recommendations from customers*. [Surprise! Not all those reviews are from real buyers!] "It is really important that people don't rush into buying an item when they spot a bargain, but take some time to make sure it is genuine first."
The charity's advice line received calls regarding 555 cases in the first three months of the year, up 17% from the same period a year earlier. They included: (1) Scam sales of items ranging from jewellery and cameras to musical instruments and driving lessons, (2) A houseboat for sale on an online marketplace, but the buyer was directed to a fake payment website and lost £5,000 as the boat was never handed over, and (3) A young man thought he was buying car insurance for £2,000 via social media after reading supposed recommendations from other buyers.
The government said that social media accounts and websites linked to scams had been closed and hundreds of arrests made. Although phantom goods only account for a fraction of scam cases, online shoppers are being urged to **avoid paying for items online via a bank transfer** [**never** pay via a bank transfer or wire transfer as you cannot recover the money], encouraged to research a trader before agreeing to a purchase, and *told to look for the padlock icon when paying online* [and *http**s** in the URL to indicate a secure site]*.

And Now, This:

Inside Peter Jackson's New Augmented Reality Studio

http://www.cartoonbrew.com/vr/inside-peter-jacksons-new-augmented-reality-studio-151959.html
[Peter Jackson and Fran Walsh are known world-wide for the creation of highly successful, leading edge film making and effects studios in New Zealand, and for “The Lord of the Rings”, “King Kong”, “The Hobbit” films, and more. Peter Jackson is the second-highest-grossing director by worldwide box office ($6.518 billion).]
At Apple's recent Worldwide Developers Conference (WWDC) in San Jose, one of the stand-out demos was from Wingnut AR, the augmented reality studio started by director Peter Jackson and his partner Fran Walsh. On stage, Wingnut AR's creative director Alasdair Coull demonstrated a tabletop ar experience made using Apple's upcoming augmented reality developer kit called ARKit and Epic Games' Unreal Engine 4. The experience blended a real world environment – the tabletop – with digital objects, in this case a sci-fi location complete with attacking spaceships, while being viewed live, on an iPad. *Cartoon Brew* asked Coull more about Wingnut AR, how the demo was made, his thoughts on opportunities for vfx and animation artists in ar, and the future of ar from the company.
Who is Wingnut AR? Based in Wellington, New Zealand, Wingnut AR was formed just over a year ago by Jackson and Walsh (Wingnut Films is the name of their film production company and the vehicle behind most of Jackson's movies). Coull told Cartoon Brew that the pair created Wingnut AR “to explore this exciting new medium and make content for the various ar platforms that are here or on the way soon.” Wellington might seem like a long way from the main location of ar and vr startups in California, but the city is of course the home base for hundreds of visual effects, animation, practical effects, sound designers, and music artists thanks to the rise of Weta Digital, Weta Workshop, and Park Road Post (Coull was himself formerly the head of R&D at Weta Digital). The team at Wingnut AR also includes games professionals, crucial for realizing real-time content in ar. [see article for much more]

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.
****