Security News Digest
March 07, 2017

- March is Fraud Prevention Month -
Take the Top Ten Scams Quiz based on the
Better Business Bureau (BBB) of Vancouver Island
Top Ten Scams for 2016

Online Security Breach at Purdy's Chocolatier Puts Private Information of Thousands of Clients at Risk

http://vancouversun.com/news/local-news/online-security-breach-at-purdys-chocolatier-puts-private-information-of-thousands-of-clients-at-risk

Vancouver-based Purdy's Chocolatier has suffered a security breach of its database that has put the private information of thousands of online clients at risk. In a notice of the data breach sent out Wednesday to clients - which was obtained by Postmedia News - *company president Peter Higgins said Purdy's was notified on Feb. 7 by one of its Internet service providers that its database, containing customers' information, was the target of a security breach*. Higgins said Friday [Mar3] that *roughly 12,000 Canadian and 1,500 U.S. buyers were impacted by the breach and that both Purdy's and the Internet company - Aptos, based in Georgia - have since taken strong measures to ensure it doesn't happen again*.

…In his note to clients, Higgins said Purdy's was told by the service provider that in late November, 2016 "an unauthorized person remotely accessed its systems and that the intrusion began in approximately February 2016 and ended in approximately December 2016." ..Higgins said *no fraudulent activity has been detected*, but the service provider told Purdy's that personal information including names, addresses, phone numbers, credit card numbers and credit card expiration dates might have been accessed. He noted that no passwords were compromised and that credit card information processed through PayPal was not accessed. Higgins said the at-risk customers represented a "cross-section" of customers who buy chocolates online. *"(The breach) was on the purdys.com site, not our shops or store locations or fundraising business that happens online or the online group purchase program." He said the company is considering its options regarding its future with Aptos*. "It's been our service provider since May 2016. We're evaluating all of our options, but haven't made our final decision (on whether or not to retain Aptos). They haven't had this problem before." Higgins said the person responsible for the security breach has not yet been identified.

University Of Moncton 'Revenge Porn' Email Attacks Targeting Female Students, Staff

http://www.huffingtonpost.ca/2017/03/03/university-of-moncton-revenge-porn_n_15141760.html

The University of Moncton says it is "working non-stop" to block malicious emails targeting a female student being sent to students and staff, although a ninth did make it through to thousands of addresses on its system. They say the email was sent late Thursday and was quickly deleted from the university's server. *The series of mass emails, some of which contained naked photos of a female student and a threat toward the university, started arriving last Saturday*. "Teams in our IT department have been working non-stop keeping watch in order to intercept the messages coming from this individual," university president Raymond Theberge said during a news conference on Friday. "The messages are difficult to block because the perpetrator uses several identities. Progress has been made over the past two days."

Theberge called the attacks a type of cyber-terrorism, but said the school wouldn't shut down its email server because that would be letting the perpetrator win. "It's never a good thing to give in to these kinds of attacks," he said. "If you give in once there will be other attacks and there will be other demands made on the institution - not only us but other institutions like us." Roxann Guerrette, president of the

university's student union, said Friday she wasn't buying Theberge's reassurances about the email system or his rationale for keeping it up and running. She said the school is looking out for its own interests instead of students and the victim. ..Guerrette has said the emails appear to be a form of blackmail or "revenge porn." She said the university has to shut down its email system to "buy time" until the attacker is found. She said the school's backup message system should be used in the meantime. ..Earlier in the week, RCMP confirmed that they had interviewed the victim and have identified a possible suspect. Sgt. Andre Pepin said Friday that no arrests have been made, but he provided no other details.

Reformed Canadian Hacker 'Mafiaboy' Teams Up with HP on Documentary About Corporate Cyberattacks

http://business.financialpost.com/category/fp-tech-desk?__lsa=0948-081c

Many companies are vulnerable to data security breaches without realizing it, so a reformed Canadian hacker wants to raise awareness about the issue and he's partnering with HP Canada on a new documentary to do it. Called *Rivolta*, the upcoming *documentary tells the story of Michael Calce - also known as "Mafiaboy" - who took down some of the world's largest e-commerce companies in 2000 at the age of 15, causing an estimated $1.7 billion in damages*. Now 32 years old and reformed, Montreal-based Calce runs a company called Optimal Secure that tries to find weak points in company networks and helps businesses understand just how vulnerable they are. *"The biggest threat from of all of this is that when I was hacking, it was about notoriety," said Calce in an exclusive interview. "Today, it is about monetary gain and I think companies need to really understand that."*

Forty per cent of Canadian companies have had a data security breach at some point, according to data by IDC. Meanwhile, *56 per cent of those breached said it happened through what seems like an unlikely source: the printer, which houses sensitive company data every day*. "Realistically, printers are the largest group of devices in an office setting and they have evolved so much," said Calce, adding that many companies just pull the device out of the box and plug it in with default settings. "Hackers can pull all of the jobs from the printer's memory or they can do many other things to run exploits like use some of the ports of the printer to gain access to the entire network."

Printers and other Internet-connected devices are one of the biggest weak links to data breaches, according to Calce. It's not just small-to-medium sized companies either, as major Fortune 250 companies are guilty of letting these devices fall through the security cracks. "The problem is huge. I go into major financial institutions that are still using default passwords on printers," said Colorado-based Michael Howard, chief security advisor and worldwide security practice lead at HP. *"Largely printers are sitting on (company networks) unmanaged and unmonitored, and they don't have any way to know if anything is going on."* Howard advises some of the biggest companies in the world to think of every device that's connected to the Internet - no matter how small - as a risk and to financially invest into proper security resources, in addition to changing the default settings.

"In Vancouver, there was a breach where (hackers) turned on a TV and recorded everything going on in a boardroom," Howard said. "Or it's also things like vending machines being put on networks." The other major vulnerability for businesses is what's called *social engineering*, according to Calce, *where hackers use things like misleading e-mails or websites to trick users into downloading software that allows a breach. The key is to be aware the problem exists and be more skeptical when something doesn't seem right*. "Nothing will ever be 100 per cent secure, but *you can mitigate the risk*," he said. "It's like driving a car… Do you buckle your seatbelt or not? You mitigate the risk of losing your life by doing so."

The upcoming documentary *Rivolta* - directed by Academy Award nominated director Hubert Davis (*Hardwood*, *Invisible City*) and produced by HP Canada - is still finalizing its release date but will take viewers through Calce's story.

[Michael Calce, along with the author of the book "Mafiaboy: How I Cracked the Internet and Why It's Still Broken", were the Closing Keynote featured at the BC government/OCIO 11th Annual Privacy and Security Conference in Victoria in February, 2010.]

North Saanich Couple Bilked of $20,000 in Email Phishing Scam, Police Say

http://www.timescolonist.com/news/local/north-saanich-couple-bilked-of-20-000-in-email-phishing-scam-police-say-1.9926743#sthash.mnhxh4Pv.dpuf

A North Saanich [Victoria area] couple has been scammed out of $20,000 in an email phishing scam, RCMP say. *The couple, in their 70s, reported that in January, they received what appeared to be a legitimate email from a Canadian bank telling them their account had been compromised*, said Sidney-

North Saanich RCMP Cpl. Doug Wilson. *The email asked for banking and personal information, which they provided*. They soon discovered that more than $20,000 had been fraudulently withdrawn from their account. *Phishing scammers often send emails at random and prompt the recipient to enter personal information into a website that looks identical to that of their financial institution*. Some scammers are purporting to be from Canada Revenue Agency and demanding overdue payments. "Of course, once the fraudsters have this information, they will very quickly use it to empty your bank accounts or rack up huge bills with credit card companies, using your name and personal financial information," Wilson said. Once the money is gone, the chances of recovering it are slim. Wilson said the best course of action is to contact your bank directly to ask if the message is legitimate. "The best way for people to protect themselves is through education so they don't fall victim to these scams in the first place," Wilson said. *[Note: Financial institutions will not contact you by email if there is a problem with your account, nor will the Canada Revenue Agency.]*

Nine Popular [Android] Password Manager Apps Found Leaking Your Secrets

http://thehackernews.com/2017/02/password-manager-apps.html

Is anything safe? It's 2017, and the likely answer is NO. Making sure your passwords are secure is one of the first lines of defense – for your computer, email, and information – against hacking attempts, and Password Managers are the one recommended by many security experts to keep all your passwords secure in one place. Password Managers are software that creates complex passwords, stores them and organizes all your passwords for your computers, websites, applications and networks, as well as remember them on your behalf.

But what if your Password Managers are vulnerable? A new report has revealed that some of the most popular password managers are affected by critical vulnerabilities that can expose user credentials. The report, published on Tuesday by a group of security experts from TeamSIK of the Fraunhofer Institute for Secure Information Technology in Germany, revealed that nine of the most popular Android password managers available on Google Play are vulnerable to one or more security vulnerabilities.

The team examined LastPass, Keeper, 1Password, My Passwords, Dashlane Password Manager, Informaticore's Password Manager, F-Secure KEY, Keepsafe, and Avast Passwords – *each of which has between 100,000 and 50 Million installs*. "The overall results were extremely worrying and revealed that password manager applications, despite their claims, do not provide enough protection mechanisms for the stored passwords and credentials," TeamSIK said. *In each application, the researchers discovered one or more security vulnerabilities – a total of 26 issues – all of which were reported to the application makers and were fixed before the group's report went public*.

According to the team, some password manager applications were vulnerable to data residue attacks and clipboard sniffing. Some of the apps stored the master password in plain text or even exposed encryption keys in the code. For example, one high severity flaw affected Informaticore's Password Manager app, which was due to the app storing the master password in an encrypted form with the encryption key hard coded in the app's code itself. A similar bug was also discovered in LastPass. In fact, in some cases, the user's stored passwords could have easily been accessed and exfiltrated by any malicious application installed on the user's device. Besides these issues, the researchers also found that auto-fill functions in most password manager applications could be abused to steal stored secrets through "hidden phishing" attacks. And what's more worrisome? Any attacker could have easily exploited many of the flaws discovered by the researchers without needing root permissions.

[Go to the article for the list of vulnerabilities disclosed in some of the most popular Android password managers by TeamSIK] *Since the vendors have addressed all these above-listed issues, users are strongly advised to update their password manager apps as soon as possible, because now hackers have all the information they require to exploit vulnerable versions of the password manager apps.*

Spam Email Operator's Faulty Backup Leaks 1.37 Billion Addresses

https://www.theguardian.com/technology/2017/mar/06/email-addresses-spam-leak-river-city-media

One of the largest spam operations in the world has exposed its entire operation to the public, leaking its database of 1.37bn email addresses thanks to a faulty backup. *As well as email addresses, the holy grail of the spam operation, personal information including real names, IP addresses and physical addresses have also been leaked, though on a smaller scale than the email information that makes up the bulk of the dataset*. According to security researchers at MacKeeper, the leaked information stems from an operation called River City Media, an email marketing firm that sends up to a billion messages a day to

spam filters across the world. “The situation presents a tangible threat to online privacy and security as it involves a database of 1.4bn email accounts combined with real names, user IP addresses, and often physical address,” said MacKeeper’s Chris Vickery. “Chances are that you, or at least someone you know, is affected.”
Vickery hasn’t managed to fully verify the leak, but says he has found addresses he knows are accurate in the database. And the source of the data, a snapshot of a backup made at some point in January 2017, accidentally published to the internet without any password protection, adds more credibility to the leak. “Well-informed individuals did not choose to sign up for bulk advertisements over a billion times,” Vickery says. “The most likely scenario is a combination of techniques. One is called *co-registration. That’s when you click on the ‘Submit’ or ‘I agree’ box next to all the small text on a website. Without knowing it, you have potentially agreed your personal details can be shared with affiliates of the site*.”
Anti-spam organisation Spamhaus, working alongside MacKeeper and Vickery, has used the information contained in the leak to add River City Media’s details to its database, blacklisting the firm’s entire infrastructure. The breach is so large that when Vickery initially reported that he had access to a leaked dataset containing 1.4bn records, India’s national government issued a statement denying that it was the source – the country’s federal ID system is one of the few databases in the world containing more than a billion individuals, and speculation ran rampant until Vickery released the actual information.

1 Million Decrypted Gmail and Yahoo Accounts Being Sold on Dark Web

https://www.hackread.com/1-million-gmail-yahoo-accounts-on-dark-web/

A dark web marketplace is where one can buy all sorts of illegal stuff including drugs, fake id cards and weapons. Lately, these marketplaces have become the best place for hackers and cyber criminals to sell databases stolen from Internet giants. A vendor going by the handle of “SunTzu583” is selling millions of Gmail and Yahoo accounts on a dark web marketplace. The listing was published this week and shows SunTzu583 is selling 100,000 Yahoo accounts acquired from Last.FM breach from 2012, in which 43 million user accounts were exposed and publicly released in September 2016. These accounts contain usernames, emails and their passwords in a plain text format. The price for this listing is only 0.0079 BTC (USD 10.75) probably because the data is already out in public.
Another listing from SunTzu583 shows more 145,000 Yahoo accounts available for sale in 0.0102 BTC (USD 13.75). These accounts also contain usernames, email and their decrypted passwords. According to HackRead’s research, these accounts were taken from two separate breaches including Adobe breach in October 2013, in which 153 million accounts were breached with each containing an internal ID, username, email, encrypted password and a password hint in plain text and MySpace breach from 2008, in which 360 million user accounts were stolen and leaked on the dark web in 2016.

Stuffed Toys Leak Millions of Voice Recordings from Kids and Parents

http://money.cnn.com/2017/02/27/technology/cloudpets-data-leak-voices-photos/index.html

Recorded messages spoken to teddy bears could pose privacy risks for children. A security vulnerability allowed anyone to view personal information, photos and recordings of children's voices from CloudPets toys. And at one point, some people tried to hold all of that information for ransom. According to a report compiled by security researcher Troy Hunt, over 820,000 user accounts were exposed. That includes 2.2 million voice recordings.
"I suspect one of the things that will shock people is that they probably didn't think through the fact that when you connect the teddy bear, your kids voices are sitting on an Amazon server," Hunt said.
CloudPets toys connect to mobile apps and let parents and loved ones send messages to their children that are played through the stuffed animals. *When you create an account with CloudPets, you give it your child's name, an email address and a photo*. Like other toys that connect to the internet, CloudPets stores all that data in the cloud, not on your smartphone itself. The toys launched in 2015, and include stuffed bears, dogs, cats and rabbits. But as Hunt and other investigators found, *kids' information was stored in an insecure database that didn't require authentication to access it*. As Hunt explained to CNNTech, it takes one mistake to expose this data - the error on the database was a bit like not having a pin on your smartphone. This database was indexed by Shodan, which is a search engine for finding insecure devices connected to the internet. You can use it to see if popular devices (like toys) are leaking data - you can also use it to take advantage of insecure systems.
According to Hunt, that's what happened. Someone deleted the data, and posted a ransom note: CloudPets would have to give the bad actors Bitcoin in order to get its data back. Instead, CloudPets

likely restored the data from a backup. *The data is no longer publicly accessible*. *But CloudPets has not informed users of the leak, and as far as researchers know, the passwords are still active*. This could be a violation of the law. In California, the government requires companies to notify users if their information was exposed online. CloudPets, and its maker Spiral Toys, are based in California.

Another Problem with the Internet of Things: Smart Home Devices Don't Work When Networks Go Down

http://globalnews.ca/news/3280756/amazon-s3-outage-smart-home-devices-wouldnt-work/

Smart home technology is pretty cool - until you're left sitting in the dark because a network outage is preventing you from turning on your wireless light bulb. *Hundreds of smart home consumers likely opened their eyes to a big problem with the Internet of Things Tuesday [Feb28], when a massive outage struck Amazon's S3 cloud storage service, disrupting service to popular websites, services and smart home networks*. The issue sent social media into a tailspin as dozens of services – including blogging site Medium, question and answer site Quora and several work productivity services, such as Trello – went down for hours.

Those with smart home products soon joined the thousands complaining about the outage, some of which laughed that they were sitting in the dark because their wireless light bulbs wouldn't turn on. One woman joked her mother had become deaf after her smart home security system wouldn't stop sounding an alarm. And anyone who owned multiple internet-connected home gadgets was really having a rough day. "AWS goes down. So does my TV remote, my light controller, even my front gate. Yay for 2017," said one user. These devices that relied on Amazon Web Servers for functionality effectively became useless during the outage. In the future, should a cloud service that other smart home companies rely on go down, these so-called smart devices could - at least temporarily - become useless bricks.

Fake Fashion Fuels Vast Illegal Profits, Funding Terrorism and Trafficking

https://www.thestar.com/business/2017/02/28/fake-fashion-fuels-vast-illegal-profits-funding-terrorism-and-trafficking.html

In a warehouse at London's sprawling Heathrow Airport, a border officer pulls open a cardboard box he suspects contains contraband goods. Bingo - his instincts are rewarded. The box is packed with beige and black sneakers that to the untrained eye look identical to the limited edition Adidas Yeezy Boost, designed by rap star Kanye West, which sold out within minutes of being released last year and now have a resale value many times their original retail price. In the past five years, the Border Force, the policing command under Britain's Home Office charged with immigration and customs controls, has seized thousands of consignments at Heathrow alone, valued at around $125 million (U.S.), said Peter Herron, senior officer for specialist operations. *"Anything a counterfeiter can counterfeit, they will."*

Annual trade in fake products was worth $461 billion in 2013, around 2.5 per cent of total global trade, according to Piotr Stryszowski, an economist with the Paris-based Organization for Economic Cooperation and Development. The money goes to organized crime, and helps fund terrorism and the trafficking of drugs, people, sex and wildlife, as well as the lavish lifestyles of its kingpins. *"It's the globalized illicit business of the 21st century,"* says Stryszowski, who laments it's not taken as seriously as other contraband, such as cocaine. Consumers may see fakes as "fun" and feel clever to buy sunglasses or sneakers that look like the real thing but cost a fraction of the price. The reality, however, is anything but fun for the workers, many of them children, who toil in appalling, often slave-like conditions in secret factories making fake products for gang bosses who, Stryszowski says, "have no ethics and no respect for the law." *It's this human cost that makes counterfeit goods one of the most insidiously dangerous criminal activities in the world today*.

London-based intellectual property lawyer Mary Bagnall describes scenes of horror - children chained to sewing machines; people locked in underground factories in remote corners of China - that characterize *an industry so lucrative yet so low-risk that some crime gangs are getting out of the drugs and people-trafficking businesses and into fakes*. "This makes more money for organized crime with less risk for them," she told The Associated Press, describing counterfeiting as part of a "massive global web" of criminality. "It's difficult to communicate to consumers why it is not a victimless crime." "Consumers are used to the idea of fake handbags and even fashion counterfeits, (which) alone amount to some 2.6 billion pounds ($3.24 billion) worth of lost sales and I think an estimated 40,000 lost jobs annually; and that's just in one industry," she said. The total annual cost to the European Union's fashion industry is $27.5 billion, she said.

Consumers can understand the perils of fake air bags for cars, or fake toys or electrical goods that "could explode in the face of a child," Bagnall said. But the fake goods industry goes much further than that. *"What consumers are probably less aware of is the danger of counterfeits in relation to other products - I'm talking now about pharmaceuticals, I'm talking about cosmetics," she said*. Ingredients found in fake cosmetics include chemicals that can cause disfigurement or worse. Medicines made on the cheap and outside regulation can cause serious health problems. "We have tested cosmetics and what we've found is that they will be containing ingredients such as cadmium, arsenic, lead, to very dangerous levels. The worst one we found contained cyanide," said Matthew Cridland, trading standards manager for Newport, a city 200 kilometres northwest of London.
The vast majority of fakes, more than 81 per cent, come from China and Hong Kong. The biggest victims are in the United States, Italy, France and Switzerland, and include designers and manufacturers of everything from high-end fashion clothing, footwear, jewelry and watches, to cosmetics, perfumes and medicines. Britain is an important destination for counterfeiters, since its purchasing power is high and its consumers enjoy buying brand-name merchandise. *Also, like many markets for fakes, the internet has seen illicit profits grow for organized crime while the risk of detection shrinks*.

Microsoft Tech Support Scam Leverages Full-Screen Mode to Trick Victims

https://www.scmagazine.com/microsoft-tech-support-scam-leverages-full-screen-mode-to-trick-victims/article/642024/
A new tech support scam website leverages deceptive visual elements to trick victims into thinking they have been redirected to a legitimate Microsoft support website, even though they actually never left the scam page. The website, to which *targets are redirected via malvertising*, uses a script from the *Techbrolo malware family* to pull off the scam, according to a Microsoft Malware Protection Center blog post. Once the page loads, victims receive both an audio alert and a pop-up message that says their computer has been locked due to a virus infection, with a fraudulent technical support number they can call for help. Clicking "OK" on the message opens what appears to be a second pop-up, as if the user is stuck in a never-ending dialogue loop (a common tech support scam tactic), but in this case the unwanted dialogue box is actually just a web element built into the page. Clicking "OK" on this element places users in full-screen mode and introduces yet another web element, designed to look like users have been redirected to the Chrome browser's version of the Microsoft support page. But it is actually still the scam site, despite what appears to be an address bar that reads "*support.microsoft.com/ru-ru/en".*
Indeed, exiting full-screen mode reveals *real* address bar, which contains a malicious URL. "As this newly discovered support scam website shows, scammers are always on the lookout for opportunities to improve their tools," the Microsoft blog post reads. "They can get really creative, motivated by the possibility of avoiding security solutions and ultimately increasing the chances of you falling for their trap."

Meet StoneDrill Malware Destroying Everything on Infected Computers

https://www.hackread.com/stonedrill-malware-destroying-everything/
The IT security researchers at Kaspersky Labs have discovered a new malware targeting oil and gas companies in the Middle East and also aiming towards targets in Europe. Dubbed StoneDrill by researchers, the malware can evade antivirus detection and destroy everything on an infected device. Kaspersky Labs discovered that StoneDrill is being used in attacks against Saudi Arabia similar to the Shamoon malware reportedly linked with Iranian government-backed hackers since 2012.
The difference between both malware is that StoneDrill is more sophisticated then Shamoon, however, its build is similar to Shamoon 2.0, a variant of Shamoon malware that made a comeback in 2016 by targeting government servers in Saudi Arabia. Also, StoneDrill and Shamoon have a different codebase yet the mindset of the authors and their programming "style" appear to be similar.
It is unclear how StoneDrill is being delivered to victims. Upon infecting a device, it injects itself into the memory process of the victim's web browser and uses two sophisticated anti-emulation techniques aimed at fooling security solutions installed on the victim machine. The malware then starts destroying the computer's disk files. Furthermore, StoneDrill also works as a backdoor apparently for large-scale espionage campaigns and spies on an unknown number of targets using four command and control (C&C) servers.
…While Shamoon malware was delivered to victims through infected documents there are chances that StoneDrill is possibly using similar means for infecting unsuspecting users. In this regards, it is highly advisable to ignore unknown emails and avoid downloading attachments and clicking links sent from unknown senders.

Consumer Reports to Consider Cyber Security in Product Reviews

http://www.reuters.com/article/us-cyber-consumerreports-idUSKBN16D0DN

Consumer Reports, an influential U.S. non-profit group that conducts extensive reviews of cars, kitchen appliances and other goods, is gearing up to start considering cyber security and privacy safeguards when scoring products. The group, which issues scores that rank products it reviews, said on Monday it had collaborated with several outside organizations to develop methodologies for studying how easily a product can be hacked and how well customer data is secured. Consumer Reports will gradually implement the new methodologies, starting with test projects that evaluate small numbers of products, Maria Rerecich, the organization's director of electronics testing, said in a phone interview. "This is a complicated area. There is going to be a lot of refinement to get this right," Rerecich said. *The effort follows a surge in cyber attacks leveraging easy-to-exploit vulnerabilities in webcams, routers, digital video recorders and other connected devices, which are sometimes collectively referred to as the internet of things*.

"Personal cyber security and privacy is a big deal for everyone. This is urgently needed," said Craig Newmark, the founder of Craigslist who sits on the board of directors at Consumer Reports. In one high-profile October attack, hackers used a piece of software known as Mirai to cripple an internet infrastructure provider, blocking access to PayPal, Spotify, Twitter and dozens of other websites for hours. Another attack in November shut off internet access to some 900,000 Deutsche Telekom customers. *Security researchers have said the attacks are likely to continue because there is little incentive for manufacturers to spend on securing connected devices*. "We need to shed light that this industry really hasn't been caring about the build quality and software safety," said Peiter Zatko, a well-known hacker who is director of Cyber Independent Testing Lab, one of the groups that helped Consumer Reports establish the standards. The first draft of the standards is available online at thedigitalstandard.org. Issues covered in the draft include reviewing whether software is built using best security practices, studying how much information is collected about a consumer and checking whether companies delete all user data when an account is terminated. Jeff Joseph, senior vice president for the Consumer Technology Association, called the decision by Consumer Reports a "positive step" but cautioned that the group "must be very clear about how they score products and the limitations of what consumers can expect."

And Now, This (the Social Psychology of IT):

How Millions of Kids are Being Shaped by Know-It-All Voice Assistants

https://www.washingtonpost.com/local/how-millions-of-kids-are-being-shaped-by-know-it-all-voice-assistants/2017/03/01/c0a644c4-ef1c-11e6-b4ff-ac2cf509efe5_story.html

Kids adore their new robot siblings. As millions of American families buy robotic voice assistants to turn off lights, order pizzas and fetch movie times, children are eagerly co-opting the gadgets to settle dinner table disputes, answer homework questions and entertain friends at sleepover parties. Many parents have been startled and intrigued by the way these disembodied, know-it-all voices - Amazon's Alexa, Google Home, Microsoft's Cortana - are impacting their kids' behavior, making them more curious but also, at times, far less polite.

In just two years, the promise of the technology has already exceeded the marketing come-ons. The disabled are using voice assistants to control their homes, order groceries and listen to books. Caregivers to the elderly say the devices help with dementia, reminding users what day it is or when to take medicine. For children, the potential for transformative interactions are just as dramatic - at home and in classrooms. *But psychologists, technologists and linguists are only beginning to ponder the possible perils of surrounding kids with artificial intelligence, particularly as they traverse important stages of social and language development*. "How they react and treat this nonhuman entity is, to me, the biggest question," said Sandra Calvert, a Georgetown University psychologist and director of the Children's Digital Media Center. *"And how does that subsequently affect family dynamics and social interactions with other people?" With an estimated 25 million voice assistants expected to sell this year* at $40 to $180 - up from 1.7 million in 2015 - there are even ramifications for the diaper crowd.

Toy giant Mattel recently announced *the birth of Aristotle, a home baby monitor launching this summer that "comforts, teaches and entertains" using AI from Microsoft*. As children get older, they can ask or answer questions. *The company says, "Aristotle was specifically designed to grow up with a child."*

Boosters of the technology say kids typically learn to acquire information using the prevailing technology

of the moment - from the library card catalogue, to Google, to brief conversations with friendly, all-knowing voices. *But what if these gadgets lead children, whose faces are already glued to screens, further away from situations where they learn important interpersonal skills? It's unclear whether any of the companies involved are even paying attention to this issue*. Amazon did not return a request for comment. A spokeswoman for the Partnership for AI, a new organization that includes Google, Amazon, Microsoft and other companies working on voice assistants, said nobody was available to answer questions.

"These devices don't have emotional intelligence," said Allison Druin, a University of Maryland professor who studies how children use technology. "They have factual intelligence." ..Today's children will be shaped by AI much like their grandparents were shaped by new devices called television. But you couldn't talk with a TV. …Naomi S. Baron, an American University linguist who studies digital communication, is among those who wonder whether the devices, even as they get smarter, will push children to value simplistic language - and simplistic inquiries - over nuance and complex questions. …And then there is the potential rewiring of adult-child communication. [see article for more]

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

****