Security News Digest
March 6, 2018

March is Fraud Awareness Month
Take our quiz and test your knowledge

This week's stories:

Close to One-Quarter of Canadians Have Clicked a Phishing Link

https://techvibes.com/2018/03/01/close-to-one-quarter-of-canadians-have-clicked-a-phishing-link

It seems that not clicking on that mystery email link in your inbox is easier said than done.

A new study from Interac shows that **nearly one-quarter of Canadians have clicked on a phishing link of some sort**, while 64 per cent reported they have been tempted to click on a link they weren't completely sure was safe. While that Nigerian prince investment opportunity may look like a good idea, it's usually a good idea to steer clear.

"As payment fraud increasingly migrates online through scams like phishing, the continued work we do with our partners to detect and prevent fraudulent activity has never been more important," said Rob Fodor, chief data scientist and VP of Fraud at Interac. "It's also why we feel strongly about arming Canadians with the information they need to spot, avoid and report any phishing scams they may come across."

March is Fraud Prevention Month, so there are a few easy ways to set yourself up and easily avoid giving away sensitive information. Some are more or less common sense, like not clicking on links from senders you don't recognize and looking for strange errors or typos in a request for information.

More in-depth information about the nature of online transactions can also help prep customers for potential fraud cases. Mobile wallets can't actually access financial information, as they are often tokenized, meaning a new credit or debit number is generated that acts as a replacement for the physical card. Paying with a debit card online also creates a one-use transaction number so businesses or hackers cannot utilize it further.

"When you're online, don't click on any links or open any attachments if you receive them from a sender you don't recognize. And trust your gut," said Fodor. "If you weren't expecting the deposit or money request notification from someone you know**, contact the sender through a different channel to check if it's real.**"

Protecting from fraud also involves checking for odd purchases and transactions that could have been compromised in another way. Offline fraud is dropping, but as more companies are attacked and suffer breaches, it can often lead to leaked information without the user being irresponsible in any way.

Another thing to look out for is accessing private information on public wifi channels, such as a coffee shop or mall. The boom of e-commerce has led to more and more people becoming too lax with their banking and password information.

Police Department Creates Zone for Safer Online Sales in Abbotsford, B.C. 

http://www.canada.com/technology/17114908/story.html

Meeting a stranger to complete an online deal can feel risky, even for a veteran police officer.

Sgt. Judy Bird knows first-hand about the "sketchy" feeling that can come with buying or selling items on platforms like Craigslist, Kijiji or Facebook. "Even though you're not doing anything wrong, it feels weird. You're sitting in your car, waiting to meet somebody that you don't know and hoping that this transaction goes well," said Bird, spokeswoman for the Abbotsford Police Department in B.C.

Abbotsford police are trying to make online deals less risky by turning two parking stalls in front of the department's headquarters into a space where people can meet safely. The area is under video surveillance and close to the station's front doors, in case safety issues arise during a deal.

"This provides one more safe place where people can meet others to make these transactions in a safer manner," Bird said. "**Most offenders will not come to the police department**." Online forums advertising everything from smart phones to wedding decor are popular in the Fraser Valley and the vast majority of transactions are problem free, she added.

But classified ads have led to violence in the past in B.C. In 2004, Marc Rozen was killed in his Vancouver apartment after he placed an ad in a local paper saying he wanted to sell an engagement ring appraised at $18,000. Police said the 38-year-old was murdered for the jewellery. A man identified by police as a gang member was convicted in 2013 of first-degree murder in Rozen's death.

Kijiji Canada spokesman Kent Sikstrom said a number of steps are taken to protect user safety on the sales platform, including technology that detects and removes potentially unsafe or illegal posts, and a customer service team that responds to listings flagged by users.

The company also encourages people to meet in public places like coffee shops to complete transactions, Sikstrom added. "If you're going to somebody's house to pick up a couch, let's say, or something heavier that you couldn't transport to a coffee shop, we always recommend bringing a friend with you, making sure you inspect the quality of the items ... maybe even agreeing to meet at those buy and sell zones as well. These are all great options," he said.

Sikstrom added that anyone who experiences a crime should report it to police. Police in Abbotsford are happy to provide a safe place for exchanges and will step in if a crime is committed, but officers can't help if an item isn't as advertised, Bird said.

People should not bring extra cash, and remember to never share personal information like social insurance numbers or banking details, she added. "Though we are a very trusting community with good people, it's important for us to also look after our own safety," Bird said.

GitHub hit with massive 1.35 Tbps DDoS attack, Could be World's Largest

https://www.techrepublic.com/article/github-hit-with-massive-1-35-tbps-ddos-attack-could-be-worlds-largest/

On Wednesday, developer repository site GitHub was hit with a critical DDoS attack that took the site offline multiple times for a few minutes each time. According to a GitHub incident report, **the attack**

peaked at 1.35 Tbps, followed by a second peak of 400 Gbps, which could make it the largest attack of its kind ever perpetrated.

According to the incident report, GitHub was offline Wednesday from 17:21 to 17:26 UTC and intermittently unavailable from 17:26 to 17:30 UTC, thanks to the attack. **The report noted that user data wasn't at risk during the attack.**

The GitHub attack is the latest in a string of incidents where hackers have exploited a vulnerability in the memcached protocol to amplify the impact of such an attack**. Memcached is typically used to speed up websites, but an issue with its UDP protocol makes the attack amplification possible**, as noted by CloudFlare.

As noted by TechRepublic contributor James Sanders, a document from the United States Computer Emergency Readiness Team (US-CERT) labels the memcached vulnerability as the most powerful known vector for amplification attacks.

Memcached, as is likely inferred by the name, is a tool that uses data caching to help ease the burden on data stores. And, as reported by ZDNet's Steve Ranger, it's not necessarily meant to be used with systems that are connected to the internet.

But, that hasn't stopped attackers from finding a way to use it to launch and accelerate cyberattacks. **By mislabeling a victim's IP as a target address, attackers can overload their network with traffic (up to 51,200x more in acceleration) and trigger a denial of service attack.**

To fix its own problem, GitHub moved some of its traffic to Akamai for additional capacity at the edge, Ranger wrote. **In its own post Akamai, one of the companies who discovered the vulnerability early on, wrote that it predicts "many more, potentially larger attacks in the near future.** Akamai has seen a marked increase in scanning for open memcached servers since the initial disclosure.

U.S. Supreme Court wrestles with Microsoft data privacy fight

https://www.reuters.com/article/us-usa-court-microsoft/u-s-supreme-court-wrestles-with-microsoft-data-privacy-fight-idUSKCN1GB0GY

Supreme Court justices on Tuesday wrestled with Microsoft Corp's dispute with the U.S. Justice Department over whether prosecutors can force technology companies to hand over data stored overseas, with some signaling support for the government and others urging Congress to pass a law to resolve the issue.

Chief Justice John Roberts and Justice Samuel Alito, both conservatives, indicated sympathy during an hour-long argument in the case toward the Justice Department's stance that because Microsoft is based in the United States it was obligated to turn over data held abroad sought by prosecutors in a U.S. warrant.

Liberal justices Ruth Bader Ginsburg and Sonia Sotomayor questioned whether the court needed to act in the closely watched case in light of Congress now considering bipartisan legislation that would resolve the legal issue.

The case began when Microsoft balked at handing over a criminal suspect's emails stored in Microsoft computer servers in Dublin in a drug trafficking case. Microsoft challenged whether a domestic warrant covered data stored abroad.

A ruling is due by the end of June, giving Congress little time to act.

"Wouldn't it be wiser to say let's leave things as they are. If Congress wants to regulate in this Brave New World,' it should do it," Ginsburg said.

Alito agreed that Congress should act but added that in the interim, something has to be done."

If the court were to rule in favor of Microsoft and Congress does not amend the 1986 law at issue in the case, Alito wondered how the government could quickly obtain information in a major criminal investigation in which data is held overseas, potentially in several different countries.

“What happens in that situation?” Alito asked.

Roberts appeared concerned that companies like Microsoft could enable customers to evade the reach of U.S. prosecutors by deliberately storing data overseas.

Microsoft might gain customers if you can assure them, no matter what happens, the government won’t be able to get access to their e-mails,” Roberts said.

The company’s lawyer, Joshua Rosenkranz, responded that customers already know that other services existed that provided stronger privacy guarantees.

Microsoft President and Chief Legal Officer Brad Smith (R) and his lawyer Josh Rosenkranz make their way to the news media to make a statement outside of the U.S. Supreme Court in Washington, U.S., “If customers do not want their e-mails to be seized by the government, they don’t use Microsoft’s services,” Rosenkranz said.

The case highlights the friction between tech companies and privacy advocates desiring to protect customer data and law enforcement wanting information vital to criminal and counterterrorism investigations

[See full article for more information]

Russian bots and trolls amplified both sides after Florida school shooting

https://globalnews.ca/news/4030346/russian-bots-and-trolls-amplified-both-sides-after-florida-school-shooting/

Russian-linked influence networks on Twitter boosted hashtags on both sides of the U.S. gun control debate in the aftermath of the Parkland, Fla., school shooting on Feb. 14, and have been doing so ever since, analysis shows.

Earlier this week, they also amplified a conspiracy theory that teenage survivor David Hogg was a “crisis actor” and part of an elaborate hoax.

On the day of the attack, they started promoting #floridashooting and #guncontrolnow as hashtags, and linking to a story that originally linked accused gunman Nikolas Cruz to a neo-Nazi organization in Florida.

By Feb. 16, they were also promoting #falseflag, a tag for arguing the shootings were faked, (at about the same frequency that they were promoting #gunreformnow, promoting gun control). On Feb. 18, as a gun-rights backlash against calls for gun control gained momentum, they started promoting #2adefenders, a gun rights tag.

By Friday, nearly two weeks after the shooting, they were promoting “Broward County” (where the shooting took place) and “Broward.” They also started promoting “Wayne LaPierre” (head of the National Rifle Association, who on Thursday launched an attack on gun control advocates, saying that they ” … hate the NRA, they hate the second amendment, they hate individual freedom“) and “LaPierre.”

They were also still promoting stories like this one, which questioned the authenticity of victims’ accounts of the shooting.

The data was gathered by Hamilton68, a project of the German Marshall Fund think-tank, which tracks about 600 troll and bot accounts it says are “linked to Russian influence operations.” Mostly, they tweet about Ukraine and Syria, but sometimes amplify the extreme right in the U.S.

It provides a real-time look at what messages Russian-linked accounts are promoting on any given day, and what debates they are trying to influence.

The pattern is several years old. The aim seems sometimes to amplify a particular side of a debate, sometimes to stoke fear and divisiveness more generally.

[See full article for more information]

15,000 internet-connected devices could be hacked to mine $1,000 of cryptocurrency in 4 days

https://www.cnbc.com/2018/03/01/thousands-of-iot-devices-can-be-hacked-to-mine-cryptocurrency-avast.html

Vulnerable internet-connected devices from security cameras to smartphones can be hijacked by hackers and turned into tools to mine cryptocurrencies, a cybersecurity company has demonstrated.

Avast, which is based in the Czech Republic, ran a demonstration on Wednesday at Mobile World Congress in Barcelona, Spain, which had a number of devices running on a network powering a cryptocurrency mining software.

Mining is the process of verifying transactions on a cryptocurrency network by solving complex mathematical problems with high-powered computers. Bitcoin is very difficult to mine without having a super computer, but another cryptocurrency called monero can be done with a network of internet-connected devices.

Avast couldn't get 15,000 devices onto its hacked network, but based on the tests it did run, it said that it would need that number of internet-connected gadgets to mine $1,000 of cryptocurrency in four days. A theoretical real-world attack would begin with hackers taking over a network of devices. They would use the combined computing power of those devices to then mine some monero.

While the $1,000 might not sound like a lot of profit, the potential is huge because in 2020, there will be over 20 billion internet-connected devices, according to a forecast by research firm Gartner, meaning the number of devices that could be attacked would be much higher. The was an estimated 8.4 billion of these devices in 2017.

"This ubiquity of devices combined with the fact they are so easy to attack makes them an attractive target," Ondrej Vlcek, the chief technology officer at Avast, told CNBC Wednesday.

Both crypto-mining and hacking of so-called internet of things devices are two rising trends. In 2016, an attack on a connected device was behind a hack that wiped out large swathes of internet access for many Americans. And North Korean government-backed hackers have been running campaigns aimed at hacking devices to mine monero.

Monero has become a favorite cryptocurrency for bad actors as it claims to be one of the most anonymous digital coins available.

And Now this:

Researchers Develop a File System for DNA-Based Storage

https://www.extremetech.com/extreme/264391-researchers-develop-file-system-dna-based-storage

Most of your cells contain a complete set of instructions to build a person stored in DNA. Scientists have worked for years on developing a storage technology that could harness the incredible density of DNA to store other types of data, but it’s been slow going. Now, a team from Microsoft Research and the University of Washington may have cracked the code to make DNA a viable storage medium.

DNA’s coding sequence is described by four base pairs: cytosine, guanine, adenine, and thymine. Those are the A,C,T, and G you always see used in DNA sequences. In your cells, bases are read three at a time, and each set of three describes a different amino acid. Put amino acids together and you get a protein. To store something else as DNA, you need to come up with a different encoding scheme, and there are several ways to do that. The real problem is how you read and retrieve the data.

To read the data you’ve encoded in DNA, you need to chop it up into shorter sequences, as there’s no way to read a full, unbroken piece of DNA. Thus, a DNA storage system needs markers that tell you

where each sequence fits. You can probably see where this is going — you have to read the entire sequence to retrieve a single file. **The work from Microsoft and the University of Washington has to do with adding random access to DNA storage. The researchers designed new sequence markers that can target specific files without accessing unneeded files.**

The key is finding enough marker sequences to tag all your files, and the team identified thousands that will work. That means you could amplify a specific sequence that identifies the files you want, and just sequence those. If you want to keep more files than you have markers, you simply have to keep additional separate pools of DNA. The other innovative tweak to DNA storage in the new study is the use of bit-flipping operation (XOR) in long strings of identical bases. DNA sequencing tends to get messy when there are too many repeated bases. The team used XOR to insert a random sequence to break up these long runs and make the data faster to read.

Microsoft Research and the University of Washington have basically described a file system for DNA. This gets us closer to using DNA for storage, but it's not likely to replace your SSD (Solid State Drive). Even with the improvements, it's slower and vastly more complicated to use than electronic storage. Still, DNA could be valuable for archival with data densities measured in hundreds of petabytes per gram.