ISSUE 6-8

BITS & BYTES

INSIDER TIPS ON HOW TO USE TECHNOLOGY TO MAKE YOUR BUSINESS RUN FASTER, EASIER AND MORE PROFITABLY

IN THIS ISSUE

August 2015

"As a business owner , I know you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems forever."

Joe Stoll, President
Technical Action Group (TAG)
JStoll@TechnicalActionGroup.com

Cybercriminals Continue To Defraud and Extort Funds From Business Victims Using Cryptowall Ransomware Schemes

The following is an announcement we found on the FBI website, posted June 23, 2015.

Source: http://www.ic3.gov/media/2015/150623.aspx

This is very relevant to Canada as well as many Canadian businesses have fallen prey to ransomware on an increasing frequency. Data from the FBI's Internet Crime Complaint Center (IC3) shows ransomware continues to spread and is infecting devices around the globe. Recent IC3 reporting identifies CryptoWall as the most current and significant ransomware threat targeting individuals and businesses. CryptoWall and its variants have been used actively to target U.S. [and Canadian] victims since April 2014. The financial impact to victims goes beyond the ransom fee itself, which is typically between $200 and $10,000. Many victims incur additional costs associated with network mitigation, network countermeasures, loss of productivity, legal fees, IT services, and/or the purchase of credit monitoring services for employees or customers. Between April 2014 and June 2015, the IC3 received 992 CryptoWall-related complaints, with victims reporting losses totaling over $18 million.

Keep in mind that most incidents go unreported. Safely assume that the damage reported above could easily be 3 or 4 times what's actually reported. An important thing to note as you read about cybercrime is that what happens in the US often happens to Canadians as well.

These financial fraud schemes target both individuals and businesses, are usually very successful, and have a significant impact on victims. The problem begins when the victim clicks on an infected advertisement, email, or attachment, or visits an infected website. Once the victim's device is infected with the ransomware variant, the victim's files become encrypted. In most cases, once the victim pays a ransom fee, he or she regains access to the files that were encrypted. Most criminals involved in ransomware schemes demand payment in Bitcoin. Criminals prefer Bitcoin because it's easy to use, fast, publicly available, decentralized, and provides a sense of heightened security/anonymity.

TIPS TO PROTECT YOUR COMPUTERS AT HOME AND WORK.....

Shiny Gadget of the Month

Navdy

Many of us realize how dangerous it is to check e-mail or text messages while we're driving, but we don't feel like we can afford to ignore our phone. Brand-new product Navdy to the rescue! Navdy is a transparent Head-Up Display (HUD) that projects information as if it's floating six feet in front of you. It's very similar to what commercial airline pilots use. Navdy works with any car, and with all iPhones and Androids.

Using the apps you already have on your phone, and with no service plans required, Navdy allows you to focus on the road and not on your phone. As a phone call comes in, Navdy's built-in camera allows you to simply swipe in midair to answer calls (or dismiss them), so you no longer have to fumble with buttons or touch screens. Plus, Navdy's voice recognition uses the voice commands you're already familiar with, whether you use Google Now or Siri.

Any notification on your phone (such as text messages or social media) can be played, read aloud or disabled, based on your preferences. Navdy even allows you to keep your teenagers safe by giving you parental controls. The product is rumored to retail at $499, but is available now for pre-order for $299. Just visit their web site at: www.navdy.com

Enable popup blockers. Popups are regularly used by criminals to spread malicious software. To avoid accidental clicks on or within popups, it's best to prevent them from appearing in the first place.

Always back up the content on your computer (at home) and servers at the office. DON'T save things on your local computer at work. Save everything on the network. If you back up, verify and maintain offline copies of your personal and application data then ransomware scams will have limited impact on you. If you are targeted, instead of worrying about paying a ransom to get your data back, you can simply have your system wiped clean and then reload your files.

Be skeptical. Don't click on any emails or attachments you don't recognize, and avoid suspicious websites altogether.

Always use antivirus software and a firewall. It's important to obtain and use business class antivirus software and firewalls from reputable companies. It's also important to continually maintain both of these through automatic updates. If you have a firewall that's more than 3 years old, or none at all, please read this article (written by TAG) to understand the important role this piece of hardware plays in protecting your business. http://www.technicalactiongroup.ca/why-you-need-to-replace-your-3-year-old-firewall

WHAT TAG IS DOING TO PROTECT OUR MANAGED CLIENTS

As part of TAG's managed security services, we provide antivirus and antimalware on each managed desktop, laptop and server. As part of our managed security practice, we are continuously proactively learning about the ever-evolving security threats (these cyber criminals have lots of time and some of them are even backed by their own governments) so we can evaluate our strategies to protect our clients against these ever evolving and increasingly sophisticated threats. Sometimes through this work we identify products that can better protect our clients than we are currently using.

Earlier this year we identified that our standard antivirus product (AVG) was not keeping up with the latest threats as it always had in the past. As a result, we searched the marketplace for a product that was more adept at protecting our clients against the latest iteration of ransomware. We landed on Kaspersky which is a best of class product for not only protecting the latest security vulnerabilities but it also uses less computer resources than its competitor AVG. For 2 months we ran it on our own computers at TAG, along with designated test machines at clients. These designated test machines are computers that our clients have tagged as usable for testing new software releases. Upon our satisfaction that Kaspersky met all the requirements and didn't pose any risk, we rolled it out to our clients in a phased in approach. While Kaspersky provides better protection, cyber criminals have a lot of time on their hands (spreading ransomware is an actual business for these people) so the threats are evolving almost daily. This creates an ongoing battle between good and evil, and all computer users still need to be wary and observe security best practices to minimize occurrences of an attack.

BETTER PROTECTION...BUT NOT BULLETPROOF

It's important to acknowledge that NO antivirus product or antimalware can 100% guarantee that you will NEVER receive a virus or malware. They do significantly reduce the chances, but computer users still need to take precautions to minimize the chances of an attack. You can have the best lock on all your home doors and windows, but give a savvy career burglar enough time, they'll get in. But investing in quality locks keeps most of them out.

Read this article **http://www.technicalactiongroup.ca/?p=1755** to learn more on why we've made the change, and the precautions that all computer users should take to minimize the chances of an attack.

What to do if you if you are alerted to an infection on your computer:

If you receive a ransomware popup or message on your device alerting you to an infection, immediately disconnect from the network to avoid any additional infections or data losses, and CONTACT TAG (or your computer support company if it's not TAG) IMMEDIATELY at 416-489-6312 x 1 in order to prevent a spread throughout your network.

The 5 Most Dangerous Pieces of Information To Give In An Email

In the book *Spam Nation*, investigative journalist and cybersecurity expert Brian Krebs revealed the single most effective (and relied upon) way cybercrime rings gain access to your bank account, credit cards and identity. Ready for it? E-mail.

Whether it's opening an attachment infected by a virus, or a phishing scam where you unknowingly give up your login to a critical web site, e-mail still remains the most popular and reliable way digital thieves can rob you blind, steal your identity and wreak havoc on your network. Worst of all? You're INVITING them in! While there are a number of things you need to do to protect yourself, here are five pieces of information you (and your team) should NEVER put in an e-mail.

1. ***Your social insurance number.*** Think of this as your "bank account" number with the government. You should never e-mail this to anyone because it can be used to open credit cards and steal your identity.

2. ***Banking information.*** Your bank account numbers, routing number and online banking login credentials should never be e-mailed. Further, avoid sending a voided, blank check as an attachment to an e-mail.

3. ***Your credit and/or debit card information.*** NEVER update a credit card via an e-mail! If you need to update a card with a vendor, there are two safe ways to do this. The first is to log in to your vendor's secured site by going to the URL and logging in. Do NOT click on a link in an e-mail to go to any web site to update your account password or credit card! Hackers are masters at creating VERY legit-looking e-mails designed to fool you into logging in to their spoof site, which LOOKS very similar to a trusted web site, to enter your username, password and other financial details, thereby gaining access. Another way to update your account is to simply CALL the vendor direct.

4. ***Login credentials and passwords.*** You should never share your passwords or answers to security questions with anyone for any site, period.

5. ***Financial documents.*** An ATTACHMENT that includes any of the above is just as dangerous to e-mail as typing it in. Never e-mail any type of financial documents (or scans of documents) to your CPA, financial advisor, bank, etc.

Remember: Banks, credit card companies and the government will never ask you to click a link to provide them with any of the five items above. If you get an e-mail requesting you to update any of

Do You Back Up Your Smartphone?

You regularly back up your computers (or at least you should), but do you do the same with your smartphone? Given the massive amounts of contact information, photos, videos and other data we all carry around on smartphones, it's critical to back them up or risk losing all that data forever. There are two basic ways to back up your phone: automatically to the cloud or manually to your computer.

To The Cloud. Cloud backups are secured with your password-protected account. They can easily be configured to run automatically so you can "set it and forget it." Apple users can use iCloud to back up photos, contacts, calendars and other data. Turn on and configure iCloud Backup by going to Settings > iCloud. Android users can back up to Google servers in much the same way, using a Google account. Configure your preferences by going to Settings > Backup.

Info@TechnicalActionGroup.com **http://www.TechnicalActionGroup.com** 416-489-6312

Change The Default Font in Word 2013

Microsoft Office changed the font size and style to Calibri 11 pt in Office 2007. For a lot of users, the size is too small, and some of you might want to change the font style as well. If you're using the new versions of Microsoft Office — either 2013 or the 2016 preview, here's how to set the default font size and style to what works best for you.

First, launch Word in 2013 and use the keyboard shortcut **Ctrl+Shift+F** to open the Font dialog box shown below. Here is where you can change the default font style, size, effects, and even the color if you want. After you choose your settings, make sure to click the **Set As Default** button in the lower left corner. If you only click OK, it will change the font for this document only.

After making your selections you'll get a confirmation dialog box where you want to select All documents based on the Normal template and click OK.

Now every time you open a document, the default font size and style will be exactly what you set it to. It's worth noting that you can use the same steps in Office 2010 too.

Unlike changing the Office color theme, which changes all of the apps in the Office suite, you need to change the default font in each app individually.

To Your Computer. Both Apple and Android users also can back up data directly to a computer manually. Generally, connecting the phone to the computer by cable is the quickest way to do this. Apple users can also use iTunes Wi-Fi Sync to wirelessly back up phone data to a computer. Remember, though, when backing up your smartphone to a computer, your data is only as safe as that computer. Be sure to back up the computer regularly as well.

Local Or Cloud: What's Best For Backup?

The option of cloud-based backup for data is a relatively recent solution. With the growing popularity of cloud-based backup, many businesses are now rushing to get on board.

You might think this is a good thing—after all, it solves a number of problems associated with local backup– but in fact, there's more to the story. Let's have a look at both sides of the backup coin.

On the one hand, using local backup for business continuity works really well for quick restores. Because both the data and the backup device are right there, it's a fast and simple solution.

However, what happens if the power goes out? Or if the device fails? Or if it gets stolen? Or if your facility is destroyed in a fire? Most likely of all, what if human error results in data loss?

The other side of the backup coin, the cloud, offers an answer: offsite copies of your data. You may think the cloud option is preferable as a result, but the fact is, cloud-only backup poses its own risks. For instance, you can't control the bandwidth. Restores tend to be difficult and time-consuming compared to restores using local backup. Finally, it bears mentioning that the cloud can fail, too.

Fortunately there's an answer, and you have been holding in your hand this whole time: the "backup coin". You don't have to flip it! The best solution is one that incorporates both sides, a hybrid cloud/local solution.

First, your data is copied and stored on a local device, so if something happens, you can do a fast and easy local restore. At the same time, your data is replicated to the cloud. If your local device fails, you'll have offsite cloud copies of your data.

In the case of a major disaster, you can spin your server up virtually and work remotely—even if your facility is destroyed.

A good business continuity plan avoids downtime. When you're down, your staff is idle wich affects the entire company: billing, fulfillment and lost sales opportunities. A staggering 90% of the total data in existence was created in the last two years; a significant portion by small business. Yet statistics show that 75% of SMB's have NO business continuity plan.

Sure, it's easy to say "I'm exempt! I don't live in a country with frequent natural disasters!" While this is true, remember you DO have employees, and a staggering 58% of downtime nationwide is caused by human error! This makes a business continuity plan critical to the success of your operations.

The goal is to say "Yes! I'm 100% sure we're covered for any disruption to our business due to downtime". If you can't say that with confidence, then we want to talk to you and help you look at options to avoid costly downtime.

Call Joseph Stoll at 416-489-6312 x 204 or JStoll@TechnicalActionGroup.com and learn how TAGuard for Business can help you be 100% sure and covered!

The Lighter Side:

Great Starting Salary

Fresh out of business school, the young man answered a want ad for an accountant. Now he was being interviewed by a highly agitated, arrogant little man who ran a small business that he had started from scratch.

"I need someone with an accounting degree," the man said. "But mainly, I'm looking for someone to do my worrying for me."

"How's that?" the would-be accountant asked.

"I worry about a lot of things," the man said. "But I don't want to have to worry about money. Your job will be to take all the money worries off my back."

"I see," the accountant said. "And how much will my position pay?"

"I'll start you at 85,000," responded the owner decisively.

"Eighty-five thousand dollars!" the accountant exclaimed. "How can such a small business afford a sum like that?"

"That," the owner said, "is your first worry. Now get to work."