TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's New

Cleanup Week in Fargo is May 1st—5th, 2017.

The annual event cleans up our cities by giving residents an opportunity to dispose of tires, appliances and other large items at no charge on their garbage collection day.

Please go to: http://cleanupweek.com for more information.

April 2017

This monthly publication provided courtesy of Rick Johnston, President of Information Management Systems

"Enabling People to Provide Great Products and Services - Anytime, Anyplace, Anywhere"

Some Ransomware Strains Are Free To Decrypt

Ransomware is everywhere. Over the last couple years, dozens of unique versions of the malware have sprung up with a singular purpose: Extorting money from your business. Before you even consider paying for the release of your data, the first thing you must always check is whether your ransomware infection already has a free cure.

The state of ransomware in 2017

It's been almost 30 years since malware was first created that could encrypt locally-stored data and demand money in exchange for its safe return. Known as ransomware, this type of malware has gone through multiple periods of popularity. 2006 and 2013 saw brief spikes in infections, but they've never been as bad as they are now.

In 2015, the FBI estimated that ransomware attacks cost victims $24 million, but in the first three months of 2016 it had already racked up more than $209 million. At the beginning of 2017, more than 10% of *all malware infections* were some version of ransomware.

Zombie ransomware is easy to defeat

Not every type of infection is targeted to individual organizations. Some infections may happen as a result of self-propagating ransomware strains, while others might come from cyber attackers who are hoping targets are so scared that they pay up before doing any research on how dated the strain is.

No matter what the circumstances of your infection are, always check the following lists to see whether free decryption tools have been released to save you a world of hurt:

Continued page 2

- Kaspersky Lab's No Ransom List
- Avast's Free Decryption Tools
- Trend Micro's Ransomware File Decryptor
- Fightransomware.com's Breaking Free List

Prevention

But even when you can get your data back for free, getting hit with malware is no walk in the park. There are essentially three basic approaches to preventing ransomware. First, train your employees about what they should and shouldn't be opening when browsing the web and checking email.

Free Decryption Tools Have Been Released To Save You A World Of Hurt

Second, back up your data as often as possible to quarantined storage. As long as access to your backed-up data is extremely limited and not directly connected to your network, you should be able to restore everything in case of an infection.

Finally, regularly update all your software solutions (operating systems, productivity software, and antivirus). Most big-name vendors are quick to patch vulnerabilities, and you'll prevent a large portion of infections just by staying up to date.

Whether it's dealing with an infection or preventing one, the best option is to always seek professional advice from seasoned IT technicians. It's possible that you could decrypt your data with the tools listed above, but most ransomware strains destroy your data after a set time limit, and you may not be able to beat the clock. If you do, you probably won't have the expertise to discern where your security was penetrated.

Don't waste time fighting against a never-ending stream of cyber attacks — hand it over to us and be done with it. Call today at 701-364-2718 or email info@imsnetworking.com to find out more information.

Turn Off Ads In Windows File Explorer

Advertisements are invading every corner of our digital lives, but if there were one place users thought they'd be safe, it'd be Windows' File Explorer. But that's no longer the case. Microsoft has started advertising products inside the window users access to navigate their hard drive. Thankfully, we know how to disable these ads.

Who is getting these ads?

Right now, we're still unsure of how widespread Microsoft's new advertising strategy goes. Not every Windows workstation has started displaying File Explorer banners, and based on some overwhelmingly negative reactions online, the campaign might get shut down before it even reaches your desktop.

However, even if you have yet to be targeted, you can quickly and easily disable these ads right now.

How do I turn them off?

At the moment, these pushy promotions show up only in Windows' File Explorer window, so that's where we'll begin. After you've opened a new window, there are only five steps to boot them off your screen:

1. Select *View* from the ribbon along the top of any File Explorer window.
2. Click *Options* on the far right-hand side.
3. In the new window select the *View* tab.
4. In the *Advanced Settings* window pane, scroll down and deselect 'Show sync provider notifications'.
5. Click *Apply* and close the Folder Options window.

That's all it takes! Keep in mind that we highly recommend the services Microsoft chose to advertise with this move. Office 365, OneDrive, and others are all great cloud platforms for safely working and collaborating from any device in any location — we just don't want to see advertisements for them when we're hunting down sales records.

Shiny New Gadget Of The Month:

Thought Oculus Was King? Think Again

Once upon a time, Oculus Rift ruled the world…

The virtual reality (VR) world, anyway. Not so much anymore. Now that VR heavyweights Sony, HTC and Samsung have entered the ring, there's a whole new reality in, well…VR.

Sony's PlayStation VR was recently crowned "Editor's Choice" by PC Mag. And, if you happen to own a compatible Samsung Galaxy smartphone, such as the S7 or S7 Edge, you can get "untethered" VR for just $100. You'll pay four times that for the Rift, HTC's Vive or Sony's PlayStation VR – all tethered sets, requiring a clunky cable from headset to hardware.

Vive has the most advanced technology, but Rift is nearly as sophisticated and sells for $200 less. You could shell out that much for the Rift's hand controllers, but, according to PC Mag, they're well worth it. So while Oculus may not be king, it's still a serious contender.

Is Fileless Malware A Threat To You?

There have been some truly horrifying cyber-security headlines popping up over the last month. If you've been reading about "fileless" malware attacking banks and other big-name institutions around the world, we're here to set the record straight: Your business isn't in direct danger. But even if you're not, staying abreast of all the details is still worthwhile.

What is this new threat?

To oversimplify the matter, fileless malware is stored somewhere other than a hard drive. For example, with some incredibly talented programming, a piece of malware could be stored in your Random Access Memory (RAM).

RAM is a type of temporary memory used only by applications that are running, which means antivirus software never scans it on account of its temporary nature. This makes fileless malware incredibly hard to detect.

This isn't the first time it's been detected

Industry-leading cyber security firm Kaspersky Lab first discovered a type of fileless malware on its very own network almost two years ago. The final verdict was that it originated from the Stuxnet strain of state-sponsored cyber warfare. The high level of sophistication and government funding meant fileless malware was virtually nonexistent until the beginning of 2017.

Where is it now?

Apparently being infected by this strain of malware makes you an expert because Kaspersky Lab was the group that uncovered over 140 infections across 40 different countries. Almost every instance of the fileless malware was found in financial institutions and worked towards obtaining login credentials. In the worst cases, infections had already gleaned enough information to allow cyber attackers to withdraw undisclosed sums of cash from ATMs.

Am I at risk?

It is extremely unlikely your business would have been targeted in the earliest stages of this particular strain of malware. Whoever created this program is after cold hard cash. Not ransoms, not valuable data, and not destruction. Unless your network directly handles the transfer of cash assets, you're fine.

If you want to be extra careful, employ solutions that analyze trends in behavior. When hackers acquire login information, they usually test it out at odd hours and any intrusion prevention system should be able to recognize the attempt as dubious.

Should I worry about the future?

The answer is a bit of a mixed bag. Cybersecurity requires constant attention and education, but it's not something you can just jump into. What you *should do* is hire a managed services provider that promises 24/7 network monitoring and up-to-the-minute patches and software updates — like us. Call today at 701-364-2718 or email info@imsnetworking.com to get started.

Bits & Bytes

As of January 31, "outsiders" can now Skype into the White House Press Room.

This enables journalists outside the Washington, DC, area to ask questions during White House press briefings. It's part of the Trump administration's strategy to keep in touch with people outside the beltway. Journalists attending via Skype must be at least 50 miles from the DC area. All political questions aside, it's just another example of business (or, in this case, government) taking advantage of available technologies. Or, in this case, finally catching up… Skype, the world's largest video calling service, is nothing new – it's been around since 2003. Sometimes it just takes a while for users to figure out how to make tech work to their advantage. *Yahoo.com*

Anti-malware programs can't even touch this new kind of attack...

"Fileless" attacks became all the rage among hackers in 2016. According to a report by cybersecurity firm Carbon Black, fourth quarter 2016 saw a 33% rise in these "non-malware" attacks compared to the first quarter. Experts expect the trend to continue through 2017. Cyberbad-guys carry out these attacks in any number of ways. Their "en vogue" method at the start of 2017 was hijacking PowerShell and WMI (Windows Management Instrumentation) to do their dirty deeds. Brian Kenyon, chief strategy officer for Symantec, said recently, "Fileless infections are difficult to detect and often elude intrusion prevention and antivirus programs." Reports show the Democratic National Committee hack last year used a fileless attack. *DarkReading.com*

Want earbuds that last and sound great?

Bragi's new earbuds, named simply The Headphone now have "bragging rights" on both battery life and sound quality. At six hours of battery life, these buds shred all competition. That includes Erato's Apollo 7 and the Earin buds – both of which wimp out at three hours. Bragi's Headphone also delivers a crystal-clear sound that beats most Bluetooth and WiFi earbuds. And they let sounds come through from whatever space you're in. They also receive phone calls and respond to voice commands. Plus, all of this is 100% wireless. They even include a sleek-looking lanyard-style carrying case. All that being said, The Headphone is well worth a look if you're looking for a great pair of earbuds.
-DigitalTrends

If you work at a standing desk, you'll love this.

Ergonomic experts agree that "your best position is your next position." In other words, your body is meant to move. And constant motion reduces fatigue as well as back and joint pain. Enter the Wurf Board, an inflatable platform for working at a standing desk. As you stand on it, your body constantly adjusts, keeping you in a subtle state of constant motion. Benefits include greater energy, focus and calorie burn. While anti-fatigue mats make standing comfortable for an hour or so, the Wurf Board lets you stand easily for hours at a time. Priced at $199-$269 and available in three sizes, it lets you work out while you work.
-TheBalance.com