

TECHNOLOGY TIMES

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

What's New

We are grateful for our partnership in 2016 and we look forward to working together in the New Year. Happy 2017!



January 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"



New Year, New Cyber-Threats

Have you had to deal with security issues in the past year? Brace yourself, as there are more to come. For this reason, security experts have become indispensable members of society, who guard tech-dependent individuals and businesses against malicious attacks that pose threats to their privacy and livelihood. As you ring in the new year, make sure you're well armed against the following predicted cyber-crimes.

Increased threats on cloud technology

Cloud service has numerous benefits to businesses. They make data storage, collaboration, and processing more efficient; they enable employees to work faster; and they help operations flow smoother. Cloud technology's popularity is expected to rise well into the next few years, but as demand increases, so does the dangers presented by cyber attackers.

Ransomware will be more complex

Ransomware incapacitates computer systems by locking down files and preventing access for ransom. In its 2016 Threat Predictions report, security software company McAfee predicts a peak in ransomware attacks next year. Although they also predict it to recede by mid-year, damages to vulnerable cloud-dependent infrastructures can be great and costly. Most alarming in the prediction, however, is that in the coming year ransomware attacks will be more complex due to new elements.

Ransomworms, which use advanced victimization techniques to mine further data within an already compromised network, are expected to put an even crueler spin to an already formidable malware. Doxing, on the other hand, affects avenues such as social media and any place where sensitive, easily

continued on page 2

Want to Lock-in your IT Costs for the Next **THREE** Years? Sign up for IMS Total Care Services **TODAY!**

identifiable information can be extracted to serve the ultimate purpose of extorting money. Yet another wicked ransomware to watch out for is Backup Deletion, which destroys the very mechanism that can otherwise help you recover from a compromised system or files: your backup data.

More threats to IoT (Internet of Things)-enabled devices

It is also predicted that 2017 will see attacks made on IoT-powered devices, which will make life harder for those who depend on technology that makes life easier. It targets medical devices and Electronic Medical Records, “connected cars”, basic domestic tools, and tech-driven wearables, such as smartwatches and fitness trackers. The danger posed by this intrusion is fully capable of corrupting information stored in your devices.

Advanced cyber espionage

Cyber espionage is by no means a novelty. In 2017, it’s expected to hold sway in cyber-threat prevention measures as it becomes even more complex. It encompasses all sectors of society, including individuals, private organizations, government institutions, and entire countries. Perpetrators will have the means to bypass networks by attacking firewalls and wreak havoc in their victims’ network. Fret not, for there will be measures in place to detect this threat also in the coming year.

Hackers are one of the most cunning criminals to have ever existed. While the cyber-police and the defenses they put up are no slouches, threats to security systems can still make technology-dependent individuals and businesses quiver. Although damaged networks can be

repaired, compromised privacy restored, and stolen data returned, the amount of damage that hackers can cause might be

irreparable and/or result in a significant dent in your IT infrastructure and budget. The value of a network security system makes itself known when you least expect it, which is why security should be a top priority.

Are you interested in learning how to educate your employees so your business doesn’t fall to hackers? For a small monthly fee you can train your staff on the latest attacks and protect your network.

What does this training include?

➤ Continuous Security Training

- Weekly Micro Security Training
- 1-2 Minute Bite-Sized Training Modules
- Ongoing Training Keeps Security Top of Mind
- Rich Multi-Media Makes

Topics Interesting

➤ Monthly Employee Security Newsletter

- Unique, Non-Technical, Magazine-style Newsletter
- Reinforces Security Training

➤ Simulated Phishing Attack Platform

- Fake Phishing Emails Test Employee Awareness
- Ability to Track and Report Employee Actions

Optional Breach Protection and Response

➤ Financial Protection and Breach Response Services

- Backed by an AIG Insurance Policy

➤ Breach Response Services Include:

- Breach Forensics, Breach Counseling, Breach Notification and Credit Monitoring to affected individuals

Let us help you protect your business and data. Give us a call at 701-364-2718 or email info@imsnetworking.com.

Shiny New Gadget Of The Month:



New Nintendo Classic Rules Them All!

For anyone in their late 20s to early 40s, chances are nothing shaped your life more than Nintendo. If it was your first “gadget,” it may even have been love at first sight.

And now, for Nintendo lovers, the Nintendo Entertainment System is back and better than ever with the NES Classic Edition. It's tiny, but designed to look just like the original NES. Setup is a snap. Just plug it into your TV's USB port. Hit the power button and you're greeted with a screen where you can browse games and options. You can even select a CRT filter that replicates the lines and look of an old TV.

The color is sharp, the timing dead on and each pixel is a perfect square so you see the games exactly as designed. At 60 bucks, it's a great gift for your favorite millennial (maybe even YOU!).

Ransomware Demands More Victims for Freedom

Popcorn Time is taking ransomware to a new level of devilish trickery by asking victims to give up two of their friends for a chance to rid their own computers of the virus. In cyber security this level of diabolical blackmail represents a new and scary trend for hackers. For more information on how Popcorn Time works and what you can do to keep it off your system, keep reading.



Ransomware is nothing new. Cybersecurity miscreants have been taking advantage of online users for years by requiring payment to “unlock” a victim's computer. What Popcorn Time does differently is give users the option to spread the virus to two other victims in the hopes that they will pay the ransom — a tactic that promises to double their money at the expense of your sense of morality (and at the expense of your friendships as well).

The Cost of Popcorn

When you inadvertently download this ransomware, you will be met with a screen that explains that your files have been hijacked/encrypted, and that to get them back you will need to pay one Bitcoin for a decryption key that they keep stored remotely. The Bitcoin fee is usually more than \$700, a hefty price to pay during any season but particularly difficult for those infected during the holiday season.

Spread the “Holiday Cheer” and Hope they Bite

What makes Popcorn Time unique is the option victims have to take their cost away by allowing the ransomware to affect two of their friends for a chance to get a free decryption code. Of course, it works only if both friends pay the ransom, which leaves you looking (and feeling) like the Grinch.

Avoiding Popcorn Time this Season

The easiest way to avoid downloading ransomware is to stay off of sites that might contain questionable files. However, this is nearly impossible for modern users, and many hackers are getting good at making their files look legitimate. Limit your exposure to potential ransomware by keeping your software up-to-date and your computer protected with a security program from a reputable company. If you need to learn more about how to avoid running into ransomware while you're online, give us a call at 701-364-2718. We'll keep you away from the popcorn this season.

Bits & Bytes

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

Here's an easy way to start 2017 with a clean e-mail in-box.

Ever wonder how in the world you ended up on so many e-mail lists? They just pile up until you can't even keep up with unsubscribing from the new ones. Unroll.me lets you manage your subscriptions by unsubscribing and bundling the ones you want to keep into

a single daily "rollup." It makes unsubscribing easy and painless. It simply lists all your subscriptions for you. You just click an X next to the ones you want to unsubscribe from and Unroll.me takes care of the rest. It's a great way to organize your in-box while keeping all the subscriptions you love.

-Lifewire.com

Imagine your team, smarter and faster in 2017.

Unlike project collaboration platforms, Asana is an app that specializes in workflow management. While it doesn't give you Gantt charts and billing information, it's one of the best tools you'll find to keep track of the daily to-do's of your business, while giving employees a more productive workspace than e-mails to track job progress. It's web-based and sports a free mobile app for iPhone and Android. And it also lets you work offline. Asana works best when one person envisions how it will work and then sets it up that way. This takes trial and error, but once up to speed, your customized version can be a powerful work tool.

-PCmag.com

Progress doesn't have to grind to a halt during an Internet outage.

First, realize how a loss of Internet access messes with people's heads. When you can't connect with people online, your primal brain feels isolated because it sees inclusion as key to survival. Then there's that little endorphin rush you start missing when you can't check a task as complete. Add to all that a fear of missing out (FOMO) when you lose touch with friends on Twitter, Facebook or e-mail, and you have a formula for widespread panic among the troops. Instead, keep your cool and carry on with these four activities: 1) Call a meeting, or do training. 2) Complete your "later" list. 3) Compose drafts. 4) Hit the streets and do some face-to-face marketing.

-Inc.com

