

TECHNOLOGY TIMES

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

What's New

Cleanup Week in Fargo is May 7th—11th, 2018.

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.

If you want more information please go to: <http://www.cleanupweek.com/Fargo.htm>



May 2018



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

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



The Shocking Truth Behind Cybercrime Threats And What You Can Do About Them Now

Today's technological innovations have empowered small businesses to do things that would have been utterly unimaginable even 15 years ago. To remain competitive in a constantly shifting landscape, we've become more dependent on software and hardware to house even the most basic structures of the companies we run.

Meanwhile, these technologies are evolving at breakneck speed. Every day, there's a slew of new devices to consider, a pile of new updates to install and a new feature to wrap our heads around. Every morning, we wake up and the digital world is thrillingly new.

But all over the world, there's an insidious network of criminals keeping up with this insanely rapid

pace of progress. With every new security measure designed to protect our digital assets, there are thousands of hackers working around the clock to determine a new way to break through. An estimated 978,000 fresh new malware threats are released into the world each day. The term “up to date” doesn't mean much anymore in the wake of new developments arriving minute by minute.

There's a price to pay for the increased efficiency and reach enabled by the digital age. We've all heard the story before. A massive, multinational corporation neglects some aspect of their security and falls victim to a crippling large-scale cyberattack, with criminals lifting millions of dollars in customer data and digital assets. Equifax, J.P. Morgan, Home Depot,

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

Yahoo!, Verizon, Uber and Target – these narratives are so commonplace that they barely raise an eyebrow when we read about them in the news.

Most business owners wrongly assume that these incidents have no bearing on their own companies, but these high-profile incidents account for less than half of data breaches. In fact, according to Verizon's 2017 Data Breach Investigations Report, 61% of attacks are directed at small businesses, with half of the 28 million small and medium-sized businesses (SMBs) in America coming under fire within the last year.

It's hard to imagine how you can possibly protect yourself from these innumerable threats. Statistically, you can be all but certain that hackers will come for your data, and there's no way to know what new tool they'll be equipped with when they do.

"We've all heard the story before. A massive, multinational corporation neglects some aspect of their security and falls victim to a large-scale, crippling cyber-attack..."

You may not be able to foresee the future, but you can certainly prepare for it. With research, education and resources, you can implement a robust security solution into the fabric of your business. That way, you can send hackers packing before they get their hooks into



the organization you've spent years building from the ground up.

One huge leap you can make right now for the security of your business is to simply realize that cyber security isn't something you can install and leave alone for years, months or even days. It requires regular updates and the attention of professionals to ensure there's no gap in your protection. There are new shady tactics being used by criminals every day, but there are also fresh protocols you can use to stave them off.

Small business owners assume that since they don't have the resources of a Fortune 500 company, they don't have the means to invest in anything but the barest of security. Obviously, hackers know this and target SMBs in droves. The bad news is that most businesses' paper-thin barriers won't save them in the event of a crisis. The good news is that it doesn't take thousands upon thousands of dollars to implement a security system that will send the hackers packing.

Contact us today at 701-364-2718 or info@imsnetworking.com if you have questions on your companies security system.



Rick attended a conference in Nashville, TN this past month. One of the guest speakers was **Kevin Mitnick!**

Kevin is an American computer security consultant, author and hacker, best known for his high-profile 1995 arrest and later five years in prison for various computer and communications-related crimes.

He now runs the security firm Mitnick Security Consulting, LLC which helps test companies' security strengths, weaknesses, and potential loopholes. He is also a Chief Hacking Officer of a security awareness training company.

Shiny New Gadget Of The Month:



This Reverse Microwave Can Quick-Freeze Food And Drinks

Way back in 1946, technology gave us the capability to pop some leftovers into the microwave and heat them up within minutes. But if we had a warm beer in our hands or needed a tray of ice quick, we were out of luck. Enter Frigondas's line of new kitchen technologies, which enable users to flash-freeze dishes, rapidly chill beverages and create crystal-clear ice within minutes. Couple this revolutionary feature with Frigondas's host of advanced heating abilities, and you've got a kitchen appliance that's set to change the microwave game for good.

The only problem is that the technology isn't yet available for purchase, with no release date in sight. Still, experts expect it to hit the market within a year or two, though it remains to be seen whether it will justify what's sure to be a hefty price tag.

Microsoft Helping With Ransomware In Office 365

Microsoft recently made small but significant changes to its Office 365 subscription service and to OneDrive, which are often used in tandem. The goal is to make it easier for users whose files have been encrypted by ransomware (or otherwise corrupted) to recover them.

The most significant of the changes is a new button that Office 365 users will see a new "File Restore" function in both applications. If you've saved your Office 365 files to OneDrive, you'll be able to restore files in a thirty-day window. In the event that your files are accidentally deleted or corrupted, getting them back is as simple as pressing the button and selecting the files to be restored.

That's a huge win for Office 365 and OneDrive users, but there's more.

The additional changes include:

- A mobile alert sent to the phone number you select, which will inform you if your files may have been encrypted or otherwise tampered with
- Support for end-to-end email encryption in their mail service (Outlook), including the web version of the mail app
- Office now scans all links embedded in PowerPoint, Excel and Word documents to check if they point to malicious content on the web
- All file attachments and links embedded in emails are now scanned for known phishing threats and viruses
- Outlook.com now gives users the ability to prevent email recipients from forwarding your emails
- The ability to password protect OneDrive shared links

That last one is also significant, and is a feature that OneDrive's user base has been clamoring on about for quite some time. OneDrive has made it incredibly easy to share files via a link-based system, but unfortunately, never offered users a way to secure those links. That, thankfully, has now changed.

Individually, all these changes are quite good, but taken together, they represent a significant step in the right direction. Kudos to Microsoft for taking the threat of ransomware so seriously, and adding specific features to help protect their users.

This article was posted in our blog, to read more click here: <https://www.imsnetworking.com/2018/04/21/microsoft-helping-with-ransomware-in-office-365/>

Bits & Bytes

■ 3 Big Trends Businesses Need To Adopt Now

When the online publication Small Business Trends surveyed nearly 500 small and midsize-business owners across the country last February, they found that technology has become more important than ever in companies of all sizes.

Though CRM is often an expensive and lofty goal for time-strapped businesses, it drastically increases growth once

it's implemented and understood. In fact, Small Business Trends found that "growing SMBs are twice as likely as their stagnant counterparts to rely on CRM in their daily lives." Along with these cohesive programs, synchronizing business data across platforms is becoming a priority as well, especially when providing a holistic view of key customer information.

Even artificial intelligence has begun to crop up in the small business market, albeit slowly. Still, it's clear that the fastest-growing businesses are using automation and predictive sale forecasting nearly twice as much as their stagnant counterparts.

SmallBusinessTrends.com, 2/14/18

■ The Internet Of Things: Are You Okay Playing Offense?

Adjusting your home's thermostat and hot water heater back to normal temperatures as you board a plane on your way home isn't just cool, it's incredibly handy. However, the network of these and other connected devices – often called "the Internet of Things" (IoT) – poses one of the biggest security problems of the modern era.

Most people think about changing their computer password regularly and their ATM PIN occasionally, but they almost never consider changing the password the programmable thermostat ships with from the factory, meaning that anyone who can access the manual has access to your thermostat.

Usually, attackers who target IoT devices don't want to cause you a problem. Instead, they use your device along with 20,000 other thermostats as "soldiers" to battle against a website or e-mail server. By flooding these sites with traffic, they can shut them down or stop your e-mail server from delivering your messages.

You should adopt a strict offensive posture against these types of threats in your life and business. If there is even a suspected problem with one of your IoT devices, pull the plug. Your heater may be cold when you get home, but at least your data will be safe.

