TECHNOLOGY TIMES

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

What's New

Did you know that October is National Cyber Security Awareness Month? We now have an online based Security Training available for our clients. During the month of October we are giving away 1 month of training for FREE to the first 5 companies that contact us! Call us today at 701-364-2718 or e-mail info@imsnetworking.com.

October 2016

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

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

Could One Tiny Leak Wipe Out Your Entire Company?

Things were going great at Michael Daugherty's up-and-coming $4 million medical-testing company.

He was a happy man. He ran a good business in a nice place. His Atlanta-based LabMD had about 30 employees and tested blood, urine and tissue samples for urologists. Life was good for this middle-aged businessman from Detroit.

Then, one Tuesday afternoon in May 2008, the phone call came that changed his life. His general manager came in to tell Daugherty about a call he'd just fielded from a man claiming to have nabbed a file full of LabMD patient documents. For a medical business that had to comply with strict federal rules on privacy, this was bad. Very bad.

It turned out that LabMD's billing manager had been using LimeWire file-sharing software to download music. In the process, she'd unwittingly left her documents folder containing the medical records exposed to a public network. A hacker easily found and downloaded LabMD's patient records. And now the fate of Michael's life – and his business – were drastically altered.

What followed was a nightmarish downward spiral for LabMD. Not one to go down without a fight, Michael found himself mired in an escalating number of multiple lawsuits and legal battles with the Federal Trade Commission and other regulators investigating the leak.

Finally, in January 2014, exhausted and out of funds, his

continued on page 2

business cratering under constant pressure, he gave up the fight and shuttered his company.

One tiny leak that could have easily been prevented took his entire company down. Could this happen to you and your business? Let's take a look at four fatal errors you MUST avoid, to make sure it never does:

"You MUST remove those accounts without delay."

Have you developed a false sense of security? Please, please, please do NOT think you are immune to a cyber-attack simply because you are not a big company. The fact is, whether you have 12 clients, or 12,000 clients, your data has value to hackers. A simple client profile with name, address and phone number sells for as little as $1 on the black market. Yet add a few details, like credit card and Social Security numbers, and the price can skyrocket – $300 per record is not uncommon. Being small doesn't mean you are immune.

Are you skimping on security to save money? Sure, of course you have a tight budget… So you cut a deal with your marketing manager, who wants to work from home at times. He links into the company network with a VPN. If configured properly, your VPN creates a secure and encrypted tunnel into your network. So his device now links his home network into the company network. The problem is, his home cable modem may be vulnerable to attack, an all-too-common issue with consumer devices. Now you have an open tunnel for malware and viruses to attack your network.

Could lack of an off-boarding process put your company at risk? It's crucial to keep a record of user accounts for each employee with security privileges. When an employee leaves, you MUST remove those accounts without delay. An internal attack by a disgruntled worker could do serious harm to your business. Be sure to close this loop.

Have you been lax about implementing security policies for desktop computers, mobile devices and the Internet? The greatest threat to your company's data originates not in technology, but in human behavior. It starts before you boot up a single device. In an era of BYOD (bring your own device), for instance, lax behavior by anyone connecting to your network weakens its security. Your team love their smartphones, and with good reason. So it's tough sticking with strict rules about BYOD. But without absolute adherence to a clear policy, you might as well sell your company's secrets on eBay.

Don't let a tiny leak sink your ship – here's what to do next…

Let us run our complete Network Security Audit for you. We'll send our top data security specialist to your location and give you a complete top-to-bottom security analysis with action plan. This is normally a $560 service. It's yours FREE when you call now through the end of October.

Don't wait until disaster strikes. Call 701-364-2718 or e-mail me at info@imsnetworking.com to schedule your FREE Network Security Audit TODAY.

Shiny New Gadget Of The Month:

Hololens: Your New Reality?

A game designer sees a moving 3-D image of a living, breathing, mace-wielding ogre – on her desk. She flicks a finger and he turns from side to side, giving her a full view of his outfit and weapons belt.

An architect looks up at the ceiling in a building he's just designed. He waves his hand and reshapes it, allowing more light through. All virtually.

A space scientist designing a Mars rover strolls through the landscape, noting from all sides the position, shape and size of rocks his vehicle must navigate.

Now it's your turn. Put on the new HoloLens by Microsoft, and what do you see? How could you use this cool new augmented reality (AR) tool in your business?

At $3,000 for the developer's version, it may not be an impulse buy. But new AR tools like this will soon be part of your computing world.

9 Cybersecurity Terms Everyone Must Know

Everyone, from doctors to lawyers, needs to continue learning to stay ahead of the times. Business owners might have it worst of all, oftentimes needing to stay on top of several industries to keep their company running. Keep reading for a refresher on all the latest trends and buzzwords used in the cybersecurity sector.

Malware
For a long time, the phrase 'computer virus' was misappropriated as a term to define every type of attack that intended to harm or hurt your computers and networks. A virus is actually a specific type of attack, or malware. Whereas a virus is designed to replicate itself, *any* software created for the purpose of destroying or unfairly accessing networks and data should be referred to as a type of malware.

Ransomware
Don't let all the other words ending in 'ware' confuse you; they are all just subcategories of malware. Currently, one of the most popular of these is 'ransomware,' which encrypts valuable data until a ransom is paid for its return.

Intrusion Protection System
There are several ways to safeguard your network from malware, but intrusion protection systems (IPSs) are quickly becoming one of the non-negotiables. IPSs sit inside of your company's firewall and look for suspicious and malicious activity that can be halted *before* it can deploy an exploit or take advantage of a known vulnerability.

Social Engineering
Not all types of malware rely solely on fancy computer programming. While the exact statistics are quite difficult to pin down, experts agree that the majority of attacks require some form of what is called 'social engineering' to be successful. Social engineering is the act of tricking *people*, rather than *computers*, into revealing sensitive or guarded information. Complicated software is totally unnecessary if you can just convince potential victims that you're a security professional who needs their password to secure their account.

Phishing
Despite often relying on face-to-face interactions, social engineering does occasionally employ more technical methods. Phishing is the act of creating an application or website that impersonates a trustworthy, and often well-known business in an attempt to elicit confidential information. Just because you received an email that says it's from the IRS doesn't mean it should be taken at face value — always verify the source of any service requesting your sensitive data.

Anti-virus
Anti-virus software is often misunderstood as a way to comprehensively secure your computers and workstations. These applications are just one piece of the cybersecurity puzzle and can only scan the drives on which they are installed for signs of well known malware variants.

Zero-day attacks
Malware is most dangerous when it has been released but not yet discovered by cybersecurity experts. When a vulnerability is found within a piece of software, vendors will release an update to amend the gap in security. However, if cyber attackers release a piece of malware that has never been seen before, and if that malware exploits one of these holes before the vulnerability is addressed, it is called a zero-day attack.

Patch
When software developers discover a security vulnerability in their programming, they usually release a small file to update and 'patch' this gap. Patches are essential to keeping your network secure from the vultures lurking on the internet. By checking for and installing patches as often as possible, you keep your software protected from the latest advances in malware.

Redundant data
When anti-virus software, patches, and intrusion detection fail to keep your information secure, there's only one thing that will: quarantined off-site storage. Duplicating your data offline and storing it somewhere other than your business's workspace ensures that if there is a malware infection, you're equipped with backups.

We aren't just creating a glossary of cyber security terms; every day, we're writing a new chapter to the history of this ever-evolving industry. And no matter what you might think, we are available to impart that knowledge on anyone who comes knocking. Get in touch with us today at 701-364-2718 or info@imsnetworking.com and find out for yourself.

Bits & Bytes

Savvy users are capitalizing on the LinkedIn–Microsoft merger.

Here are three ways you too can profit: 1) Your profile photo now appears on both platforms. Run it by photofeeler.com to make sure it's up to snuff. 2) When it comes to updates, forget text – video rules. Check your newsfeed and you'll see how LinkedIn puts video on top and is burying articles. No wonder members have seen a 60% to 90% drop in readership. To get attention, go video. 3) Keep an eye on LinkedIn's social advertising. With access to user data from both platforms, your ads could now enjoy a wider audience of both LinkedIn and Microsoft users. This merger opens new doors for users. Now's the time to capitalize on it.

-*Entrepreneur*

Want to know the secret to beating ransomware?

If there's one pop-up you NEVER want to see on your computer screen, it's this: "Your files have been encrypted. You have 72 hours to submit payment or they will be deleted forever." Once ransomware hits, it's too late. Game over. The best way to beat ransomware is prevention. Make sure it never happens in the first place. And if somehow it happens anyway, make sure you have up-to-date backups ready to go. The first step to prevention is to invest in serious cybersecurity. Start with antivirus software with active monitoring. Then, layer in anti-malware and anti-ransomware programs. Finally, store current backups in the cloud and/or on a separate unplugged hard drive.

-*blog.malwarebytes.com*

A wafer-thin laptop so light you'll forget it's in your briefcase…

Want an ultrasleek machine with enough battery life to keep you going long hours without plugging in? A new breed of "ultraportables" offers that and more. The lightning-quick storage on these units lets you resume work in seconds, even after they've been idle or asleep for days. The "best in breed" will cost you a pretty penny. But if you're willing to spend a little, you can get premium features. Touch screens, full HDMI ports and eight hours or more of battery life are not uncommon. At the top end, you can expect a high-resolution 4K screen (3840 x 2160). Be extra-nice and Santa might even slip one in your stocking!

-*PCmag.com*

Considering Facebook Live Video for your business?

Using Facebook Live is brain-dead simple. If you haven't already, install the Facebook app on your smartphone. Open it up, tap the red "Go Live" icon and you're on. It tells you how many are watching, plus their names and comments. When you're done, it saves to your Timeline. And, unlike Snapchat or Periscope, it doesn't disappear after just 24 hours. You can share, embed, Tweet – or delete – to your heart's content. And you can filter who sees it. As for content? Interview key employees, big shots in your niche or your customers. Share how you're making a new product. Or how your team relaxes. Why do it? Your customers love getting that little peek "behind the scenes."

-*PostPlanner.com*

HACKERS ARE PEOPLE TOO!

If you merely scan the headlines from popular news cycles, you might be led to believe in a false narrative about hackers. In truth, a hacker is simply someone with an advanced understanding of computers and networks. Unfortunately, that word has been used irresponsibly by the media for decades, resulting in a negative image which unfairly groups bad guys with good guys. To be clear, all hackers are not criminals; only criminal hackers are criminals.

Want to learn more about the hacker community? Check out these two documentaries ***Hackers Are People Too*** *and* ***DEFCON: The Documentary!***

THIS *IS* A HACKER:

In the 1996 movie *Independence Day* with the world is attacked by aliens. David Levinson (Jeff Goldblum) successfully breached the aliens' network by reading satellite transmissions of their communications. His brilliant idea to stop the aliens from eradicating Earth was to attack their network by "giving it a cold"—a computer virus—that would disable their shields. Levinson and Capt. Steven Hiller (Will Smith) socially engineered their way into the mothership by disguising themselves as aliens and flying an alien aircraft up to the ship. Essentially, this was a real life version of a phishing attack. Levinson uploads his virus to the mothership, which ultimately disables the force fields of all the alien ships (denial of service).

In short, a hacker saved the world.

THIS IS *NOT* A HACKER:

From 2005 to 2007, a man by the name of Albert Gonzalez carried out the biggest fraud in history by stealing and reselling 170 million credit card and ATM numbers. Gonzalez and his crew targeted the payment systems and networks of major corporations such as T.J. Maxx and Barnes & Noble, among many others. Gonzalez was eventually arrested, and is currently serving a 20-year prison sentence.

Gonzalez is not a hacker. He's a criminal. Even if he used hacking techniques, and obviously has advanced computer know-how, as soon as he used his skills to break the law and harm his fellow citizens, he became a criminal.