TECHNOLOGY TIMES

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

Luck Is For Leprechauns — Is Your Business Prepared for Future Security Threats?

If your business hasn't been the target of malicious intruders or cybercriminals, consider yourself lucky. Hackers are a relentless bunch and they want your gold: information and access they can use to exploit loopholes in your business's Internet security. The last few years have been hard on companies all across the globe. And these cyber-breaches aren't going to stop simply because the "damage has been done." In the US and Canada, reported incidents have affected over 215 million consumers and over 7 million small businesses. And that's only counting the attacks that authorities have uncovered.

For cybercriminals, there is no end game. All too often, small business owners assume they are outside the firing line and hackers aren't interested in them. While the media focuses on the big cyber-attacks, there are countless other stories playing out at small businesses everywhere. Cybercriminals are constantly in search of loopholes and weak security. And, unfortunately, small businesses often have the weakest IT security.

Security industry analysts predict that 2015 won't be much different from 2014 when it comes to cyber-security. There are going to be more data breaches. It's just a matter of where and when. It's also a matter of being prepared.

During the month of March, we are offering local businesses a FREE Cyber-Security Audit to help uncover loopholes in your company's online security. At no cost or obligation, our highly trained team of IT pros will come to your office and conduct this comprehensive audit. And after we're done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and a Prioritized Plan Of Attack for getting any problems addressed fast.

Because of the intense one-on-one time required to deliver these Cyber-Security Audits, we can only extend this offer to the first seven lucky companies who request it by March 17th—St. Patrick's Day. All you have to do is call our office at 701-364-2718.

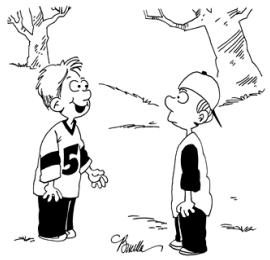
"Enabling People to Provide Great Products and Services - Anytime, Anyplace, Anywhere"

- Rick Johnston, Information Management Systems

March 2015

Fargo, ND

Inside This Issue...



"You know what I just noticed about playing outside? No pop-up windows."

HIPAA Settlement Underscores The Vulnerability Of Unpatched And Unsupported Software

Anchorage Community Mental Health Services (ACMHS) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule with the Department of Health and Human Services (HHS), Office for Civil Rights (OCR). ACMHS will pay $150,000 and adopt a corrective action plan to correct deficiencies in its HIPAA compliance program. ACMHS is a five-facility, nonprofit organization providing behavioral health care services to children, adults, and families in Anchorage, Alaska.

OCR opened an investigation after receiving notification from ACMHS regarding a breach of unsecured electronic protected health information (ePHI) affecting 2,743 individuals due to malware compromising the security of its information technology resources. OCR's investigation revealed that ACMHS had adopted sample Security Rule policies and procedures in 2005, but these were not followed. Moreover, the security incident was the direct result of ACMHS failing to identify and address basic risks, such as not regularly updating their IT resources with available patches and running outdated, unsupported software.

"Successful HIPAA compliance requires a common sense approach to assessing and addressing the risks to ePHI on a regular basis," said OCR Director Jocelyn Samuels. "This includes reviewing systems for unpatched vulnerabilities and unsupported software that can leave patient information susceptible to malware and other risks."

ACMHS cooperated with OCR throughout its investigation and has been responsive to technical assistance provided to date. In addition to the $150,000 settlement amount, the agreement includes a corrective action plan and requires ACMHS to report on the state of its compliance to OCR for a two-year period.

Want more information on becoming HIPAA compliant? Contact our office today 701-364-2718 or info@imsnetworking.com

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/acmhs/acmhsbulletin.pdf

The Truth About E-mail In 2015

Love it, hate it or call it the gold at the end of your rainbow, e-mail is here to stay. Over the past two decades, it's become deeply ingrained in our day-to-day business communication. It's basically a requirement. Despite a number of software advances and changes in the online communication landscape, e-mail is more important than ever.

This was recently confirmed by a study conducted by Pew Research. They found that e-mail is indispensable among those who are Internet-connected at work. These days, that covers a lot of people. In fact, 61% say it plays an integral role in their job. Additionally, 46% say e-mail access keeps them more productive (while another 46% say e-mail has no bearing on their productivity one way or the other). Only 7% say e-mail hurts their productivity.

In 2014, social media analysts warned that e-mail was on its last legs and that it would soon be overtaken by other online services. However, as this study seems to confirm, that is not the case. In fact, in the workplace, it's very much the opposite. The Pew study found that social media, including Facebook, LinkedIn and Twitter, benefited only about 4% of those in a connected workplace.

Even among the millennial generation, and those who regularly use social media networks in their personal lives, it hasn't been something fully translatable to the professional environment as a productivity factor. This doesn't discount uses for social media in the workplace—as a marketing or customer outreach tool—but no social media platform has come close to replacing e-mail as the go-to communication tool.

That doesn't mean Silicon Valley start-ups aren't trying. They are always at work trying to find that next four-leaf clover in online communication, hoping to develop that so-called "e-mail killer." So far, nothing has stepped up that can achieve what e-mail can, particularly for businesses.

For many businesses, it comes right back to the fact that e-mail works. It's a proven platform and it remains the business communication "golden child." It's the same reason phones and fax machines aren't extinct. They serve a purpose and they help us get things done. That doesn't stop businesses from always looking for ways to streamline that process.

Another reason e-mail works: accessibility. E-mail is used on nearly a universal level. Social media platforms, while many are incredibly popular, can't touch the truly global reach of e-mail. Have you considered how e-mail impacts your job? Does it keep you productive? Or are you ready to move on to the Next Big Thing?

Shiny New Gadget Of The Month:

The Withings Activité Pop

Lately, it seems the tech world has been inundated with wearable devices, from fitness trackers to smartwatches. They offer a number of useful features, but they also lack in elegance. They are often bulky, ordinary, complicated and—in the case of smartwatches—have less than desirable battery life.

This is where the Withings Activité Pop comes in. It looks like a classy watch on the outside, but on the inside it's a very different story. It's an activity tracker, verging on expressing itself as a smartwatch.

From the smartphone app, you control everything, from the analog dials to your activity goals. The watch face features a secondary dial that tracks your activity—from 0% to 100%—for the day. It's simple and straightforward. It's water-resistant up to 30 meters and available in three colors: azure, sand and shark gray. It's currently available at Best Buy, in-store and online.

FRAUD ALERT—Phishing Attack Warning

The email was sent from a non-Wells Fargo email address 'on behalf' of Wells Fargo and warned that the client's account had been frozen.

WELLS FARGO

Dear Customer,
Your account has been frozen temporarily in order to protect it .
The account will continue to be frozen until it is approved and validate your account information.
To proceed to confirm your account information please follow the instructions that will be required.
1. Download the attached document and open it with your browser.
2. Confirm that you are the account holder and follow the instructions.
Thank you.
Wells Fargo Customer Care

The document attached to the email was a web file that requested that the user enter the following information, which was then submitted to a 'bad guy website'. When they submitted the information, they received an error message that the page was unavailable, but that does not mean that the information wasn't actually sent to the bad guys. It could be that the bad guys wanted to give a sense of relief to the victim that they hadn't actually sent off all of their personal information to the bad guys.

Enter your username and password to securely view and manage your Wells Fargo accounts online.

*Username :
*Password :

Please enter your information.
*First Name :
*Last Name :
*Date of Birth : Day Month Year
*SSN Number :
*ATM Pin :

Mandatory Field*

The web form that was attached to the email pulled much of its content from Wells Fargo's actual website, so it appeared to be a legitimate email request.

PLEASE NOTE: No company that you do business with will ever send you an email asking you to enter all of your private information and send it to them to unlock your account (or for any other reason for that matter). If you are in question, please call your business partner and speak with their customer support department or just delete the email.

Never Forget A Password Again With A Password Manager

We all have a number of passwords for all the online services we use. You name it: banking, online bill payment, e-mail, social networks, shopping and more. You know it's incredibly easy to lose track of them all—unless you are committing one of the greatest online security offenses by using one password for everything.. One of the best—and most secure—ways to handle your passwords is with a password manager.

It's not uncommon for password managers to get overlooked when it comes to online security. There is a lingering—and false—concern that keeping all of your passwords in one place can potentially open up all your protected accounts to intruders—if they are able to break into the password manager. It's a legitimate concern, but password managers use powerful encryption to keep your passwords safe. They are specifically designed to keep you even more secure than you otherwise would be.

Many password managers—including LastPass, KeePass and 1Password—do much more than simply "remember" your passwords. They also offer password- creation assistance. They will tell you if a password is too weak or just right. Some managers offer the option to generate a secure password for you. Since you don't need to remember it, it can be more complex. They are compatible with a number of platforms and they are packed with customizable tools to keep you safe.

IMS Total Care Services Clients—How to Create a Ticket using the IMS Tray Icon

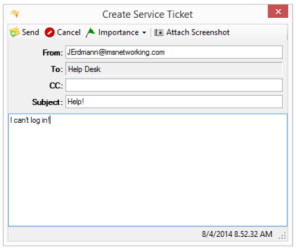
Need Support Assistance or have Questions?

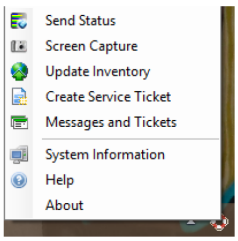
If you can't find a file, need a program installed, are having any computer problems, or have any questions, you can email help@imsnetworking.com.

You can also open a ticket right from the system tray on any computer that has our IMS TCS agent installed. This will send an alert to all IMS technicians.

To open a ticket:

1. Find the IMSTCS tray icon (Life Preserver icon), left click on it and select "Create ServiceTicket"
2. Fill out the necessary information, and be sure to click "Attach Screenshot" so the technician can see a screenshot of what is going on right away.
3. Click Send. It can take up-to 5 minutes for the IMS staff to be notified.
4. For Immediate Assistance please call our Help Desk at (701) 364-2718.





The Lighter Side:

Endorse This Skill: Jihad

We endorse the skills of our coworkers, friends, acquaintances and other connections on LinkedIn all the time. But what would you do if one of your connections listed "jihad" as one of his skills? Unless you're in the business of extremism (you're probably not), you're likely to slink away quietly and alert LinkedIn admins.

Well, one senior Taliban commander decided to update his LinkedIn profile with this very "skill." Specifically, he listed "jihad and journalism." This particular terrorist leader, Ehsanullah Ehsan, even lists himself as "self-employed."

Unfortunately (or fortunately), when LinkedIn was contacted by the *Telegraph* for further information, the social media company decided it was best to take the account down.

There has been some chatter as to the legitimacy of the account. The profile's distinct lack of Taliban propaganda and recruiting information suggested it wasn't operated by the terrorist leader himself or anyone in a significant leadership position.

Of course, as a terrorist leader and all-around terrible human being, he has more pressing things to worry about other than a suspended LinkedIn account, such as a $1 million bounty placed on him by Pakistani officials.